

# Khôlles de Mathématiques

Kylian Boyet, George Ober, Hugo *Vangilluwen*

2 juin 2024

## Résumé

Bienvenue très chers camarades sereins, ce document contient les questions de khôlles de mathématiques de la MP1 de Fermat. Il est coécrit par Kylian Boyet, George Ober, Hugo *Vangilluwen* (qui maintient la structure du projet, la compilation et le paquet `kholles.sty`) avec la contribution de Jérémie Menard. Il n'est malheureusement pas exhaustif. Si vous voulez nous aider, lisez `CONTRIBUER.md` et envoyez-nous votre code `LATEX` ou plus simplement dites-nous quand vous rencontrez une erreur.

## Table des matières

<b>1</b>	<b>Semaine 1</b>	<b>1</b>
1.1	Preuve formelle de la somme des entiers et des termes d'une suite géométrique . . .	1
1.2	Preuve de la factorisation de $a^n - b^n$ puis de celle de $a^{2m+1} + b^{2m+1}$ . . . . .	1
1.3	Développement d'une somme . . . . .	2
1.4	Preuve de la formule du binôme de Newton . . . . .	2
1.5	Montrer que tout entier $n > 2$ admet un diviseur premier . . . . .	3
1.6	Montrer par récurrence qu'une fonction polynomiale à coefficients réels est nulle si et seulement si tous ses coefficients sont nuls . . . . .	4
1.7	Montrer par analyse/synthèse qu'une fonction réelle d'une variable réelle s'écrit de manière unique comme somme d'une fonction paire et d'une fonction impaire . . .	5
1.8	Illustration graphique de certaines identités trigonométriques . . . . .	5
1.9	Technique de résolution des équations trigonométriques du type $A \cos x + B \sin x = C$	5
1.10	Étude complète de la fonction tangente, tracé du graphe et en déduire celui de cotangente. . . . .	6
1.11	Expression $\sin \theta$ , $\cos \theta$ , $\tan \theta$ en fonction de $\tan \frac{\theta}{2}$ . . . . .	6
1.12	Preuve des formules du type $\cos p + \cos q = \dots$ . . . . .	7
<b>2</b>	<b>Semaine 2</b>	<b>8</b>
2.1	Montrer qu'une composée d'applications inj/surj/bij est inj/surj/bij . . . . .	8
2.2	Montrer que, si $u$ est une application de $E$ dans $F$ , si $v$ est une application de $F$ dans $E$ telle que $v \circ u = \text{Id}_E$ et $u \circ v = \text{Id}_F$ alors $u$ est bijective ( $v$ aussi) et sa bijection réciproque est $v$ . . . . .	8
2.3	Montrer que $v \circ u$ injective implique $u$ injective + montrer que cela n'implique pas $v$ injective. . . . .	8
2.4	Montrer que $v \circ u$ surjective implique $v$ surjective + montrer que cela n'implique pas $u$ surjective. . . . .	9
2.5	Soit $u$ une application de $E$ dans $F$ . Si $A$ et $A'$ sont des parties de $E$ , y'a-t-il égalité entre $u(A \cap A')$ et $u(A) \cap u(A')$ ? (On justifiera les réponses aux deux inclusions suggérées par la question) . . . . .	9
2.6	Montrer que, si $u$ est une application de $E$ dans $F$ . Si $B$ est une partie de $F$ , alors $u^{-1}(F \setminus B) = E \setminus u^{-1}(B)$ . . . . .	9
2.7	Montrer que, parmi les entiers ne s'écrivant qu'avec des 7, il existe au moins un multiple de 61. . . . .	10
<b>3</b>	<b>Semaine 3</b>	<b>11</b>
3.1	Preuve de l'inégalité triangulaire et de l'inégalité montrant que le module est 1-lipschitzien + dessin et interprétation géométrique . . . . .	11
3.2	Caractérisation du cas d'égalité de l'inégalité triangulaire dans $\mathbb{C}$ . . . . .	11
3.3	Calcul de $\sum_{k=0}^n \cos(k\theta)$ pour tout $\theta \in \mathbb{R}$ . . . . .	11
3.4	Si $z_0$ est racine de la fonction polynômiale $P$ , alors $P$ se factorise par $(z - z_0)$ . . .	12

3.5	Si $z_1, \dots, z_n$ sont $n$ racines distinctes de la fonction polynômiale $P$ de degré $n$ , alors $P(z)$ se factorise en ...	13
3.6	Calculer le module et un argument de $z = 1 + e^{i\theta}$ en fonction de $\theta \in [0, 2\pi[$	13
3.7	Décrire (avec preuve) l'ensemble des racines $n$ -ièmes de l'unité et les localiser géométriquement dans le plan complexe.	14
3.8	Somme et Produit des racines $n$ -ièmes	14
<b>4</b>	<b>Semaine 4</b>	<b>16</b>
4.1	Résolution des équations algébriques de degré 2 dans $\mathbb{C}$ et algorithme de recherche d'une racine carrée sous forme cartésienne (sur un exemple explicite).	16
4.2	Résolution de $e^z = z_0$ où $z_0 \in \mathbb{C}^*$	17
4.3	Montrer l'unicité de l'élément neutre et du symétrique d'un élément sous des hypothèses sur la loi à préciser.	17
4.4	Preuve de la caractérisation d'un sous-groupe, application au fait que $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$ .	18
4.5	Si $\varphi$ est un morphisme de groupes de $G_1$ de neutre $e_1$ dans $G_2$ de neutre $e_2$ , calculer $\varphi(e_1)$ et $\varphi(x^{-1})$	18
4.6	Montrer que l'image d'un sous-groupe par un morphisme de groupes est un sous-groupe du groupe d'arrivée	19
4.7	Montrer que l'image réciproque par un morphisme de groupes d'un sous-groupe est toujours un sous-groupe du groupe de départ,	19
<b>5</b>	<b>Semaine 5</b>	<b>20</b>
<b>6</b>	<b>Semaine 6</b>	<b>21</b>
6.1	Montrer que si $f$ est impaire et bijective, alors $f^{-1}$ est aussi impaire. Donnez un/des exemples.	21
6.2	Limite (et preuve) lorsque $x$ tend vers $+\infty$ de $\frac{(\ln x)^\alpha}{x^\beta}$ pour $\alpha, \beta \in (\mathbb{R}_+^*)^2$ .	21
6.3	Limite en 0 de $\frac{1-\cos(x)}{x^2}$ et limite en $+\infty$ suivant $n$ de $\frac{(q^n)^\alpha}{(n!)^\beta}$ pour $q \in \mathbb{R}$ et $(\alpha, \beta) \in (\mathbb{R}_+^*)^2$	22
6.4	Présentation exhaustive de la fonction arcsin.	24
6.5	Présentation exhaustive de la fonction arccos.	24
6.6	Présentation exhaustive de la fonction arctan.	25
6.7	2 preuves de $\arcsin(x) + \arccos(x) = \frac{\pi}{2}$ sur $[-1, 1]$ , dont une basée sur une interprétation géométrique du cercle trigonométrique.	26
6.8	Présentation analytique rapide des fonctions cosh et sinh.	27
<b>7</b>	<b>Semaine 7</b>	<b>28</b>
7.1	Calcul de $\int_0^{2\pi} e^{imt} dt$ en fonction de $m \in \mathbb{Z}$ . En Dédurre qu'une fonction polynômiale nulle sur un cercle centré en l'origine a tous ses coefficients nuls.	28
7.2	Preuve de la Linéarité de la dérivation d'une fonction complexe	29
7.3	Dérivée composée d'une fonction à valeurs complexes	29
7.4	Caractérisation des fonctions dérivables de dérivée nulle sur un intervalle	29
<b>8</b>	<b>Semaine 8</b>	<b>30</b>
8.1	Preuve de l'expression des solutions réelles des EDL homogènes d'ordre 2 à coefficients constants réels dans le cas $\Delta < 0$ (en admettant la connaissance de l'expression des solutions à valeurs complexes des EDL2 à coeff. constants).	30
8.2	Existence et unicité d'une solution au problème de Cauchy pour les EDL d'ordre 2 à coefficients constants et second membre continu sur $I$ (cas complexe puis cas réel).	30
8.3	Les solutions d'une EDL2 constituent un espace vectoriel.	32
8.4	Formules de Cramer pour les systèmes $2 \times 2$	32
<b>9</b>	<b>Semaine 9</b>	<b>35</b>
9.1	Deux classes d'équivalence sont disjointes ou confondues. Les classes d'équivalence constituent une partition de l'ensemble sur lequel on considère la relation d'équivalence.	35
9.2	Si $A$ admet un plus grand élément c'est aussi sa borne supérieure. Si $A$ admet une borne supérieure dans $A$ c'est son plus grand élément.	35
9.3	Théorème de la division Euclidienne dans $\mathbb{Z}$	36
9.4	Une suite décroissante et minorée de nombres entiers relatifs est stationnaire	36

<b>10 Semaine 10</b>	<b>37</b>
10.1 Caractérisation de la densité d'une partie $A$ de $\mathbb{R}$ dans une partie $B$ de $\mathbb{R}$ la contenant avec des $\varepsilon$ .	37
10.2 Théorème de la division pseudo-euclidienne dans $\mathbb{R}$	37
10.3 $\mathbb{Q}$ est dense dans $\mathbb{R}$ et $\mathbb{R} \setminus \mathbb{Q}$ est aussi dense dans $\mathbb{R}$	38
10.4 Preuve de l'unicité de la limite d'une suite convergente	38
10.5 Une suite convergente est bornée	39
<b>11 Semaine 11</b>	<b>40</b>
11.1 Caractérisation séquentielle de la densité.	40
11.2 Théorème de la convergence monotone	40
11.3 Théorème de Césarò	41
11.4 Théorème de passage à la limite dans une inégalité.	42
11.5 Théorème des suites adjacentes	42
11.6 <i>Facultative</i> Théorème de Bolzano-Weierstrass	42
11.7 <i>Facultative</i> Caractérisation de la convergence par l'unicité d'une valeur d'adhérence pour une suite bornée.	43
<b>12 Semaine 12</b>	<b>45</b>
12.1 Résolution d'une relation de récurrence linéaire d'ordre 1 à coefficients constants et avec second membre	45
12.2 Résolution d'une relation de récurrence linéaire homogène d'ordre 2 à coefficients constants dans $\mathbb{C}$ lorsque l'équation caractéristique possède un discriminant non nul	45
12.3 Caractérisation de la convergence par l'unicité d'une valeur d'adhérence pour une suite bornée.	46
12.4 Monotonie de $u$ et des sous-suites des termes pairs et impairs de la suite $u_{n+1} = f(u_n)$ selon la monotonie de $f$	47
12.5 L'intérieur de l'ensemble des rationnels est vide.	47
12.6 Théorème sans nom version continue au voisinage de $a$	47
<b>13 Semaine 13</b>	<b>49</b>
13.1 Théorème de composition des limites	49
13.2 Théorème des valeurs intermédiaires	49
13.3 Théorème de Weierstraß	50
<b>14 Semaine 14</b>	<b>52</b>
14.1 Expression de dérivées successives	52
14.2 Dérivé d'une bijection réciproque	52
14.3 Dérivée d'un extremum local intérieur au domaine de définition	53
14.4 Théorème de Rolle et formule des accroissements finis	53
14.5 Inégalité des accroissements finis	54
14.6 Caractère lipschitzien d'une fonction $\mathcal{C}^1$ sur un segment	56
14.7 Théorème du prolongement de la propriété de la dérivabilité	56
14.8 La fonction $\zeta$ (pas celle-là une autre) est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$	56
<b>15 Semaine 15</b>	<b>58</b>
15.1 Inégalité de Jensen	58
15.2 Inégalité arithmético-géométrique	59
<b>16 Semaine 16</b>	<b>60</b>
16.1 Unicité de la partie régulière d'un développement limité	60
16.6 Deux fonctions équivalentes au voisinage de $a$ ont le même signe sur un voisinage de $a$	60
16.7 Condition nécessaire et suffisante pour qu'une fonction $\mathcal{C}^\infty$ admette un extremum local ou un point d'inflexion	61
<b>17 Semaine 17</b>	<b>62</b>
17.4 Théorème de Bézout	62
17.6 Théorème de Gauss	62
17.8 Résoudre une équation du type $ax + yb = c$	62

<b>18 Semaine 18</b>	<b>64</b>
18.1 L'ensemble des nombres premiers est infini . . . . .	64
18.2 Caractérisation de la valuation $p$ -adique . . . . .	64
18.3 Caractérisation de $a b$ par les valuations $p$ -adiques et preuve de leur propriété de morphisme. . . . .	64
18.4 Expression du pgcd et du ppcm à partir des décomposition en facteurs premiers de $a$ et $b$ . . . . .	65
18.5 Pour $p$ premier, $(a + b)^p \equiv a^p + b^p \pmod{p}$ , en déduire le petit Th. de Fermat (2 versions), expression du résultat dans $\mathbb{Z}/p\mathbb{Z}$ . . . . .	65
18.6 $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n$ est premier. . . . .	66
18.7 Les éléments inversibles d'un anneau $A$ forment un groupe multiplicatif noté $(A^\times, \times)$	66
18.8 L'image directe par un morphisme d'anneau d'un sous-anneau de l'anneau de départ est un sous anneau de l'anneau d'arrivée. De même pour l'image réciproque. . . . .	67
<b>19 Semaine 19</b>	<b>68</b>
19.1 $(A \times B)^T = B^T \times A^T$ . . . . .	68
19.2 Calculer $E^{i,j} \times E^{k,l}$ en fonction de $i, j, k, l$ et des symboles de Kronecker . . . . .	68
19.3 Les matrices triangulaires supérieures forment un sous-anneau de $\mathcal{M}_n(\mathbb{K})$ . . . . .	69
19.4 Si $A$ est une matrice d'ordre $n$ et $\lambda$ un scalaire non nul d'un corps, alors la transposée de $A$ et $\lambda A$ sont inversibles aussi. . . . .	69
19.5 Si $N$ est une matrice d'ordre $n$ nilpotente, alors $I_n + \lambda N$ est inversible pour tout $\lambda$ , scalaire d'un corps. . . . .	69
19.6 Caractérisation de l'inversibilité pour les matrices . . . . .	69
19.7 Caractérisation des matrices diagonales inversibles . . . . .	70
<b>20 Semaine 20</b>	<b>71</b>
20.1 Éléments inversibles de l'anneau $\mathbb{K}[X]$ . . . . .	71
20.2 Théorème d'interpolation de lagrange . . . . .	71
20.3 Formule de Taylor dans $\mathbb{K}[X]$ (caractéristique nulle) . . . . .	72
20.4 Caractérisation de la multiplicité d'une racine . . . . .	73
20.5 Identification de $\mathbb{K}[X]$ à $\mathbb{K}[x]$ , par l'injectivité de $\Phi$ . . . . .	74
20.6 Pour $P = (X - x_1)(X - x_2)(X - x_3)$ , exprimer $x_1^3 + x_2^3 + x_3^3$ en fonction des fonctions symétriques élémentaires . . . . .	74
20.7 Expression de $S_2, S_{-1}$ et $S_{-2}$ à l'aide des fonctions élémentaires symétriques. . . . .	75
<b>21 Semaine 21</b>	<b>76</b>
21.1 Caractérisation des polynômes irréductibles de degré 1, 2 et 3 dans $\mathbb{K}[X]$ . . . . .	76
21.2 Polynômes irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$ . . . . .	76
21.3 $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$ . . . . .	76
21.4 PGCD d'un polynôme de $\mathbb{C}[X]$ et son polynôme dérivé . . . . .	77
21.5 Justifier la bonne définition de la dérivée d'une fraction rationnelle. . . . .	77
21.6 Théorème de Gauss-Lucas et interprétation graphique. . . . .	78
21.7 Deux expressions du coefficient associé à un pôle simple dans une décomposition en éléments simples. . . . .	78
21.8 Expressions des deux coefficients associés à un pôle double dans une décomposition en éléments simples. . . . .	79
<b>22 Semaine 22</b>	<b>81</b>
22.1 Caractérisation d'une famille liée . . . . .	81
22.2 Caractérisations d'une base . . . . .	81
22.3 Le noyau et l'image d'une application linéaire sont des sous-espaces vectoriels . . . . .	82
22.4 L'image par une application linéaire d'une partie génératrice engendre l'image de l'application linéaire . . . . .	83
22.5 Caractérisation inj/surj/bij d'une application linéaire par l'image d'une base de l'espace de départ. . . . .	83
22.6 Caractérisation d'une application linéaire par l'image d'une base . . . . .	84
<b>23 Semaine 23</b>	<b>86</b>
23.1 L'ensemble des automorphisme d'un espace vectoriel muni de la loi de composition forme un groupe . . . . .	86
23.2 Caractérisation de la somme directe de $p$ sous-espaces vectoriels . . . . .	86

<b>24 Semaine 24</b>	<b>87</b>
24.1 Existence d'un supplémentaire en dimension finie . . . . .	87
24.2 Dimension de $\mathcal{L}_{\mathbb{K}}(E, F)$ . . . . .	87
24.3 Formule de Grassman . . . . .	87
24.4 Caractérisation injectivité/bijektivité/surjectivité par le rang . . . . .	88
24.5 Théorème du rang . . . . .	89
24.6 Rang d'une composition d'applications linéaires . . . . .	89
24.7 Caractérisation des hyperplans . . . . .	89
24.8 Proportionnalité des formes linéaires ayant le même noyau . . . . .	90
24.9 Intersection d'hyperplans . . . . .	91
<b>25 Semaine 25</b>	<b>93</b>
25.1 S'il existe un inverse à droite (ou à gauche) pour une matrice carrée, alors celle ci est inversible . . . . .	93
<b>26 Semaine 26</b>	<b>94</b>
<b>27 Semaine 27</b>	<b>95</b>
27.1 Norme uniforme d'une fonction continue par morceaux . . . . .	95
27.2 Lemme d'approximation uniforme d'un fonction continue sur un segment par une fonction en escalier . . . . .	95
<b>28 Semaine 30</b>	<b>97</b>
28.7 Dénombrement des surjections de $\llbracket 1; n \rrbracket$ dans $\llbracket 1; 2 \rrbracket$ et dans $\llbracket 1; 3 \rrbracket$ . . . . .	97
28.8 Lemme des bergers . . . . .	97

# 1 Semaine 1

## 1.1 Preuve formelle de la somme des entiers et des termes d'une suite géométrique

*Démonstration.*     $\diamond$  Soit  $n \in \mathbb{N}$  fq. Posons

$$S_n = \sum_{k=0}^n k$$

En posant la symétrie d'indice  $i = n - k$ , on a aussi

$$S_n = \sum_{i=0}^n (n - i) = \sum_{i=0}^n n - \sum_{i=0}^n i = (n \times \text{card}[[0, n]]) - \sum_{i=0}^n i$$

Or, puisque  $\text{card}[[0, n]] = n + 1$  et que  $\sum_{i=0}^n i = S_n$

$$S_n = n \times (n + 1) + S_n$$

Donc

$$S_n = \frac{n(n+1)}{2}$$

$\diamond$  Soient  $q \in \mathbb{R}$ ,  $k \in \mathbb{N}$  fixés quelconques.

★ Si  $q = 1$ ,

$$\sum_{i=0}^k q^i = \sum_{i=0}^k 1 = k + 1$$

★ Sinon, avec l'identité algébrique, on a

$$q^{k+1} - 1^{k+1} = (q - 1) \sum_{i=0}^k q^i \times 1^{k-i}$$

Ainsi, puisque  $q \neq 1$  on a, par multiplication par  $(q - 1)^{-1}$

$$\sum_{i=0}^k q^i = \frac{q^{k+1} - 1}{q - 1}$$

Nous avons donc établi que

$$\sum_{i=0}^k q^i = \begin{cases} \frac{1-q^{k+1}}{1-q} & \text{si } q \neq 1 \\ k + 1 & \text{sinon} \end{cases}$$

□

## 1.2 Preuve de la factorisation de $a^n - b^n$ puis de celle de $a^{2m+1} + b^{2m+1}$

*Démonstration.* Calculons

$$\begin{aligned} (a - b) \sum_{k=0}^{m-1} a^k b^{m-1-k} &= a \sum_{k=0}^{m-1} a^k b^{m-1-k} - b \sum_{k=0}^{m-1} a^k b^{m-1-k} \\ &= \sum_{k=0}^{m-1} a^{k+1} b^{m-1-k} - \sum_{k=0}^{m-1} a^k b^{m-k} \end{aligned}$$

Si bien qu'en posant le changement d'indice  $j = k + 1$  on reconnaît le télescope.

$$\sum_{j=1}^m a^j b^{m-j} - \sum_{k=0}^{m-1} a^k b^{m-k} = a^m - b^m$$

□

### 1.3 Développement d'une somme

$$\left(\sum_{k=1}^n x_k\right)^2 = \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n}} x_k x_j = 2 \sum_{\substack{1 \leq k < j \leq n}} x_k x_j + \sum_{k=1}^n x_k^2$$

*Démonstration.*

$$\begin{aligned} \left(\sum_{k=1}^n x_k\right)^2 &= \left(\sum_{k=1}^n x_k\right) \times \left(\sum_{j=1}^n x_j\right) \\ &= \sum_{k=1}^n \left[ x_k \times \sum_{j=1}^n x_j \right] \\ &= \sum_{k=1}^n \left( \sum_{j=1}^n x_k \times x_j \right) \\ &= \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n}} x_k x_j \end{aligned}$$

On peut aussi séparer cette somme

$$\begin{aligned} \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n}} x_k x_j &= \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k < j}} x_k x_j + \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k=j}} x_k x_j + \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k > j}} x_k x_j \\ &= \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k < j}} x_k x_j + \underbrace{\sum_{k=1}^n x_k^2}_{\text{somme sur les indices } (k,j) \text{ tels que } k=j} + \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k > j}} x_k x_j \end{aligned}$$

On remarque aussi qu'en permutant les indices des deux sommes (les variables sont muettes)

$$\sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k < j}} x_k x_j = \sum_{\substack{1 \leq j \leq n \\ 1 \leq k \leq n \\ j < k}} x_j x_k$$

Qui, par commutativité du produit dans  $\mathbb{C}$  nous donne cette égalité

$$\sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k < j}} x_k x_j = \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k > j}} x_k x_j$$

On a donc bien l'identité attendue :

$$\sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k < j}} x_k x_j = 2 \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n \\ k < j}} x_k x_j + \sum_{k=1}^n x_k^2$$

□

### 1.4 Preuve de la formule du binôme de Newton

Pour tout  $(a, b) \in \mathbb{C}^2$ ,  $n \in \mathbb{N}$  :

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

*Démonstration.* Soient  $(a, b) \in \mathbb{C}^2$  fixés quelconques. Posons le prédicat  $\mathcal{P}(\cdot)$  défini pour tout  $n \in \mathbb{N}$  par

$$\mathcal{P}(n) : (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

- ★ Initialisation,  $n \leftarrow 0$  D'une part  $(a + b)^0 = 0$ , même si les deux sont nuls (par convention  $0^0 = 0$ ) D'autre part

$$\sum_{k=0}^0 \binom{0}{k} a^k b^{n-k} = \binom{0}{0} a^0 b^0 = 0$$

Donc  $\mathcal{P}(0)$  est vérifiée.

- ★ Soit  $n \in \mathbb{N}$  fixé quelconque tel que  $\mathcal{P}(n)$  est vraie

$$\begin{aligned} (a + b)^{n+1} &= (a + b) \times (a + b)^n \\ &= (a + b) \times \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \\ &= a \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} + b \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \\ &= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n+1-k} \\ &= \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n+1-j} + \sum_{k=0}^n \binom{n}{k} a^k b^{n+1-k} \end{aligned}$$

$$(\text{en posant } j = k + 1) = a^{n+1} + \sum_{j=1}^n \binom{n}{j-1} a^j b^{n+1-j} + \sum_{k=1}^n \binom{n}{k} a^k b^{n+1-k} + b^{n+1}$$

$$= a^{n+1} + \left( \sum_{k=1}^n \left( \binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} \right) + b^{n+1}$$

$$(\text{en utilisant la relation de Pascal}) = a^{n+1} + \sum_{k=1}^n \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1}$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$$

Donc  $\mathcal{P}(n + 1)$  est vraie.

□

## 1.5 Montrer que tout entier $n > 2$ admet un diviseur premier

*Démonstration.* Raisonnons par récurrence forte avec la propriété  $\mathcal{P}(\cdot)$  définie pour tout  $n > 2$  par

$$\mathcal{P}(n) : \forall k \in \llbracket 2, n \rrbracket, k \text{ admet un diviseur premier}$$

— Initialisation :  $n \leftarrow 2$

Soit  $k \in \llbracket 2, 2 \rrbracket$  fixé quelconque. Nécessairement,  $k = 2$ . or, 2 admet 2 pour diviseur premier.

Donc  $\forall k \in \llbracket 2, 2 \rrbracket, k$  admet un diviseur premier, ce qui prouve  $\mathcal{P}(2)$ .

— Hérédité : Soit  $n \in \mathbb{N} \setminus \{1, 0\}$  fixé quelconque tel que  $\mathcal{P}(n)$  est vraie.

Pour montrer  $\mathcal{P}(n+1)$ , il nous faudra montrer que  $\forall k \in \llbracket 2, n+1 \rrbracket, k$  admet un diviseur premier

Soit  $k \in \llbracket 2, n+1 \rrbracket$  fixé quelconque.

- ★ Si  $k \in \llbracket 2, n \rrbracket$ , alors la véracité de  $\mathcal{P}(n)$  nous permet de conclure, et de dire que  $k$  admet un diviseur premier.

- ★ Sinon  $k = n + 1$

◇ Si  $n + 1$  est premier, alors il admet  $k$  comme diviseur premier



◇ Sinon,  $\exists d \in \llbracket 2, n \rrbracket : d \mid n + 1$

Mais, puisque  $d \in \llbracket 2, n \rrbracket$ , la véracité de  $\mathcal{P}(n)$  nous permet d'affirmer que  $d$  admet un diviseur premier  $p$ . Donc par transitivité de la relation de divisibilité

$$(p \mid d \text{ et } d \mid n) \implies p \mid n$$

□

## 1.6 Montrer par récurrence qu'une fonction polynomiale à coefficients réels est nulle si et seulement si tous ses coefficients sont nuls

*Démonstration.* Considérons le prédicat  $\mathcal{P}(\cdot)$  défini pour tout  $n \in \mathbb{N}$

$\mathcal{P}(n)$  : toute fonction polynômiale identiquement nulle sur  $\mathbb{R}$  a tous ses coefficients nuls

Autrement dit

$$\mathcal{P}(n) : \forall (a_0, \dots, a_n) \in \mathbb{R}^{n+1} \left( \forall x \in \mathbb{R}, \sum_{k=0}^n a_k x^k = 0 \right) \implies \forall k \in \llbracket 0, n \rrbracket, a_k = 0$$

◇ Pour  $n \leftarrow 0$  Soit  $a_0 \in \mathbb{R}$  fixé quelconque tel que  $\forall x \in \mathbb{R}, a_0 x^0 = 0$  Alors  $a_0 = 0$

◇ Soit  $n \in \mathbb{N}$  fixé quelconque tel que  $\mathcal{P}(n)$  est vraie Soient  $(a_0, \dots, a_{n+1}) \in \mathbb{R}^{n+2}$  Posons  $Q(x) = \sum_{k=0}^{n+1} a_k x^k$  tel que  $\forall x \in \mathbb{R}, Q(x) = 0$  D'une part

$$\forall x \in \mathbb{R}, \underbrace{Q(2x)}_{=0} - 2^{n+1} \underbrace{Q(x)}_{=0} = 0$$

D'autre part

$$\begin{aligned} \forall x \in \mathbb{R}, Q(2x) - 2^{n+1} Q(x) &= \sum_{k=0}^{n+1} a_k (2x)^k - 2^{n+1} \sum_{k=0}^{n+1} a_k x^k \\ &= \sum_{k=0}^{n+1} a_k (2^k - 2^{n+1}) x^k \end{aligned}$$

Le terme d'indice  $n + 1$  s'annule, si bien que l'on peut écrire

$$\forall x \in \mathbb{R}, Q(2x) - 2^{n+1} Q(x) = \sum_{k=0}^n a_k (2^k - 2^{n+1}) x^k$$

Qui est une fonction polynômiale de degré  $\leq n$ , ce qui permet d'appliquer  $\mathcal{P}(n)$  pour  $(a_k)_{k \in \llbracket 0, n \rrbracket} \leftarrow (a_k (2^k - 2^{n+1}))_{k \in \llbracket 0, n \rrbracket}$ .

Donc  $\forall x \in \llbracket 0, n \rrbracket : a_k (2^k - 2^{n+1}) = 0$  et puisque  $2^k - 2^{n+1} \neq 0$ , on en déduit que

$$\forall k \in \llbracket 0, n \rrbracket, a_k = 0$$

L'expression de  $Q$  devient :

$$\forall x \in \mathbb{R}, \underbrace{\sum_{k=0}^n a_k x^k}_{=0} + a_{n+1} x^{n+1} = 0$$

Donc en particulierisant pour  $x \leftarrow 1$ , on en déduit que  $a_{n+1} = 0$

Donc  $\mathcal{P}(n + 1)$  est vraie.

□

## 1.7 Montrer par analyse/synthèse qu'une fonction réelle d'une variable réelle s'écrit de manière unique comme somme d'une fonction paire et d'une fonction impaire

*Démonstration.* Soit  $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$  fixée quelconque.

◇ Analyse : Supposons que  $f : \mathbb{R} \rightarrow \mathbb{R}$  se décompose de manière unique en  $f = g + h$  avec  $g$  paire et  $h$  impaire (i.e.  $\forall x \in \mathbb{R}, g(-x) = g(x)$  et  $h(-x) = -h(x)$ ). Soit  $x \in \mathbb{R}$  fixé quelconque. Calculons  $f(-x)$  :

$$f(-x) = g(-x) + h(-x) = g(x) - h(x)$$

Par demi somme, nous avons donc

$$\begin{cases} 2g(x) = f(x) + f(-x) \\ 2h(x) = f(x) - f(-x) \end{cases}$$

Ainsi, si une telle décomposition existe, c'est

$$\begin{cases} g : x \mapsto \frac{f(x)+f(-x)}{2} \\ h : x \mapsto \frac{f(x)-f(-x)}{2} \end{cases}$$

◇ Synthèse : Posons

$$g \left| \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto \frac{f(x)+f(-x)}{2} \end{array} \right. \quad \text{et} \quad h \left| \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto \frac{f(x)-f(-x)}{2} \end{array} \right. \quad (1)$$

Remarquons, d'une part que :

$$\forall x \in \mathbb{R}, g(x) + h(x) = \frac{f(x) + f(-x)}{2} + \frac{f(x) - f(-x)}{2} = f(x)$$

Vérifions si les fonctions  $g$  et  $h$  vérifient les conditions de parité :

$$\forall x \in \mathbb{R}, g(-x) = \frac{f(-x) + f(-(-x))}{2} = \frac{f(x) + f(-x)}{2} = g(x) \text{ ainsi } g \text{ est paire.}$$

$$\forall x \in \mathbb{R}, h(-x) = \frac{f(-x) - f(-(-x))}{2} = -\frac{f(x) - f(-x)}{2} = -h(x) \text{ ainsi } h \text{ est impaire}$$

□

## 1.8 Illustration graphique de certaines identités trigonométriques

*Démonstration.*

□

## 1.9 Technique de résolution des équations trigonométriques du type $A \cos x + B \sin x = C$

*Démonstration.* Étudions l'équation d'inconnue  $x$

$$A \cos x + B \sin x = C$$

★ Si  $A = 0$  et  $B = 0$

◇ Si  $C = 0$  l'équation admet  $\mathbb{R}$  pour ensemble de solutions

◇ Sinon, l'équation n'admet pas de solutions

★ Sinon,

Factorisons par  $\sqrt{A^2 + B^2}$  (ce qui a un sens car  $(A, B) \neq (0, 0) \implies \sqrt{A^2 + B^2} \neq 0$ )

$$\frac{A}{\sqrt{A^2 + B^2}} \cos x + \frac{B}{\sqrt{A^2 + B^2}} \sin x = \frac{C}{\sqrt{A^2 + B^2}}$$

Le nombre complexe  $\frac{A}{\sqrt{A^2 + B^2}} + i \frac{B}{\sqrt{A^2 + B^2}}$  est de module 1, donc  $\exists \varphi \in \mathbb{R}$  tel que

$$e^{i\varphi} = \underbrace{\frac{A}{\sqrt{A^2 + B^2}}}_{\cos \varphi} + i \underbrace{\frac{B}{\sqrt{A^2 + B^2}}}_{\sin \varphi}$$

Ainsi,

$$(\cos \varphi \cos x - \sin \varphi \sin x) = \frac{C}{\sqrt{A^2 + B^2}}$$

donc

$$\cos(\varphi + x) = \frac{C}{\sqrt{A^2 + B^2}}$$

$$\diamond \text{ Si } \frac{C}{\sqrt{A^2 + B^2}} \leq 1$$

$$\begin{aligned} \cos(\varphi + x) = \frac{C}{\sqrt{A^2 + B^2}} &\iff \begin{cases} \phi + x \equiv \arccos \frac{C}{\sqrt{A^2 + B^2}} [2\pi] \\ \text{ou} \\ \phi + x \equiv -\arccos \frac{C}{\sqrt{A^2 + B^2}} [2\pi] \end{cases} \\ &\iff x \in \bigcup \begin{cases} \left\{ \arccos \frac{C}{\sqrt{A^2 + B^2}} + 2k\pi \mid k \in \mathbb{Z} \right\} \\ \left\{ -\arccos \frac{C}{\sqrt{A^2 + B^2}} + 2k\pi \mid k \in \mathbb{Z} \right\} \end{cases} \end{aligned}$$

$\diamond$  Sinon, l'équation n'admet aucune solution

□

## 1.10 Étude complète de la fonction tangente, tracé du graphe et en déduire celui de cotangente.

*Démonstration.*

□

## 1.11 Expression $\sin \theta$ , $\cos \theta$ , $\tan \theta$ en fonction de $\tan \frac{\theta}{2}$

*Démonstration.* Soit  $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$ . Posons  $u = \tan \frac{\theta}{2}$

$$\diamond \tan \theta = \frac{2u}{1-u^2}$$

En utilisant la formule classique de trigonométrie

$$\tan(a+b) = \frac{\tan a + \tan b}{1 - \tan a \tan b}$$

On obtient, avec  $(a, b) \leftarrow (\frac{\theta}{2}, \frac{\theta}{2})$

$$\tan \theta = \frac{2 \tan \frac{\theta}{2}}{1 - \tan^2 \frac{\theta}{2}} = \frac{2u}{1-u^2}$$

$$\diamond \cos \theta = \frac{1-u^2}{1+u^2}$$

$$\begin{aligned} \cos \theta &= 2 \cos^2 \frac{\theta}{2} - 1 \\ &= \frac{2}{1 + \tan^2 \frac{\theta}{2}} - 1 \\ &= \frac{2}{1 + u^2} - 1 \\ &= \frac{1-u^2}{1+u^2} \end{aligned}$$

$$\diamond \sin \theta = \frac{2u}{1+u^2}$$

$$\begin{aligned} \sin \theta &= \cos \theta \tan \theta \\ &= \frac{1-u^2}{1+u^2} \times \frac{2u}{1-u^2} \\ &= \frac{2u}{1+u^2} \end{aligned}$$

□

### 1.12 Preuve des formules du type $\cos p + \cos q = \dots$

*Démonstration.* Partons des formules d'addition

$$\cos(a+b) = \cos a \cos b - \sin a \sin b$$

$$\cos(a-b) = \cos a \cos b + \sin a \sin b$$

$$\cos(a+b) + \cos(a-b) = 2 \cos a \cos b \quad (\spadesuit)$$

Si bien qu'en posant

$$\begin{cases} p = a+b \\ q = a-b \end{cases} \iff \begin{cases} a = \frac{p+q}{2} \\ b = \frac{p-q}{2} \end{cases}$$

D'où, en injectant dans ()

$$\cos p + \cos q = 2 \cos \frac{p+q}{2} \cos \frac{p-q}{2}$$

□

## 2 Semaine 2

### 2.1 Montrer qu'une composée d'applications inj/surj/bij est inj/surj/bij

*Démonstration.* Soient  $u : E \rightarrow F$  et  $v : F \rightarrow G$

◇ Supposons  $u$  et  $v$  injectives.

Soient  $(x_1, x_2) \in E^2$  fq tels que  $(v \circ u)(x_1) = (v \circ u)(x_2)$ .

Alors  $v(u(x_1)) = v(u(x_2))$ , mais  $v$  est injective donc,  $u(x_1) = u(x_2)$  mais  $u$  est injective donc  $x_1 = x_2$ . Ainsi  $v \circ u$  est injective.

◇ Supposons  $u$  et  $v$  surjectives Soit  $y \in G$  fixé quelconque.

$v$  est surjective donc  $\exists t \in F : v(t) = y$

$u$  est surjective, donc  $\exists x \in E : u(x) = t$  Ainsi,

$$(v \circ u)(x) = v(u(x)) = v(t) = y$$

Donc  $v \circ u$  est surjective.

◇ Supposons  $u$  et  $v$  bijectives.

Le fait que  $v \circ u$  est une bijection est une conséquence des deux points précédents.

□

### 2.2 Montrer que, si $u$ est une application de $E$ dans $F$ , si $v$ est une application de $F$ dans $E$ telle que $v \circ u = \text{Id}_E$ et $u \circ v = \text{Id}_F$ alors $u$ est bijective ( $v$ aussi) et sa bijection réciproque est $v$

*Démonstration.* Soient  $(u, v) \in \mathcal{F}(E, F) \times \mathcal{F}(F, E)$  qui satisfont les conditions de l'énoncé.

◇  $u$  est injective

Soient  $(x_1, x_2) \in E^2$  fixés quelconques tels que  $u(x_1) = u(x_2)$ . Alors  $v(u(x_1)) = v(u(x_2))$ .

Donc  $x_1 = x_2$  puisque  $v \circ u = \text{Id}_E$

◇  $u$  est surjective Soit  $y \in F$  fixé quelconque. Posons  $t = v(y)$ . Ainsi,  $u(t) = u(v(y)) = y$  car  $u \circ v = \text{Id}_F$

Ainsi,  $u$  est bijective, notons  $u^{-1}$  sa bijection réciproque

$$u^{-1} \circ (u \circ v) = (u^{-1} \circ u) \circ v$$

$$u^{-1} \circ \text{Id}_F = \text{Id}_E \circ v$$

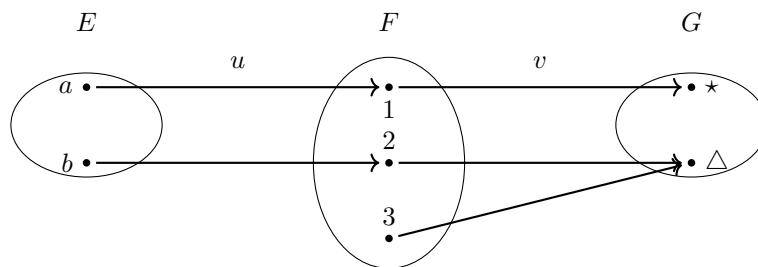
$$u^{-1} = v$$

□

### 2.3 Montrer que $v \circ u$ injective implique $u$ injective + montrer que cela n'implique pas $v$ injective.

*Démonstration.* Soient  $(u, v) \in \mathcal{F}(E, F) \times \mathcal{F}(F, G)$ .

Supposons  $v \circ u$  est injective Soient  $(x_1, x_2) \in E^2$  fixés quelconques tels que  $u(x_1) = u(x_2)$ . Composons par  $v$  à gauche :  $v \circ u(x_1) = v \circ u(x_2)$  Puisque  $v \circ u$  est injective, cela implique que  $x_1 = x_2$ .



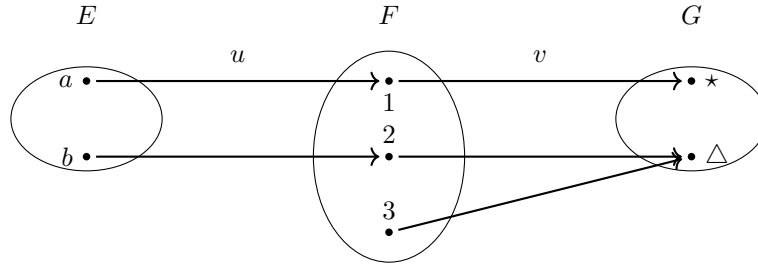
Ici,  $v \circ u$  est injective, on a montré que cela impliquait  $u$  injective. Pourtant,  $v$  n'est pas injective.

□

## 2.4 Montrer que $v \circ u$ surjective implique $v$ surjective + montrer que cela n'implique pas $u$ surjective.

*Démonstration.* Soient  $(u, v) \in \mathcal{F}(E, F) \times \mathcal{F}(F, G)$ .

Supposons  $v \circ u$  est surjective. Soit  $y \in G$  fixé quelconque. Puisque  $v \circ u$  est surjective,  $\exists x \in E : (v \circ u)(x) = y$ . Donc  $v(u(x)) = y$ . Donc, en posant  $t = u(x)$ , on a  $v(t) = y$ . Ainsi,  $v$  est surjective.



Ici,  $v \circ u$  est surjective, on a montré que cela impliquerait  $v$  surjective. Pourtant,  $u$  n'est pas surjective. □

**Remarque :** Les deux contre-exemples exhibés ici sont les mêmes, mais il y en a bien d'autres où  $v \circ u$  n'est pas bijective.

## 2.5 Soit $u$ une application de $E$ dans $F$ . Si $A$ et $A'$ sont des parties de $E$ , y'a-t-il égalité entre $u(A \cap A')$ et $u(A) \cap u(A')$ ? (On justifiera les réponses aux deux inclusions suggérées par la question)

*Démonstration.* Soit  $u \in \mathcal{F}(E, F)$  fixée quelconque,  $(A, A') \in \mathcal{P}(E)^2$ , deux parties de  $E$ .

◇ Soit  $y \in u(A \cap A')$  fixé quelconque. Par définition  $\exists x \in (A \cap A') : u(x) = y$ . Ainsi,  $x \in A \implies u(x) \in u(A)$  et  $x \in A' \implies u(x) \in u(A')$ . Donc  $y \in u(A) \cap u(A')$ .

$$\left. \begin{array}{l} u(x) \in u(A) \\ u(x) \in u(A') \end{array} \right\} \implies u(x) \in u(A) \cap u(A')$$

Donc  $u(A \cap A') \subset u(A) \cap u(A')$ .

◇ En revanche l'inclusion réciproque est fautive : considérons

$$u \left| \begin{array}{ll} \{1, 2, 3, 4\} & \rightarrow \{a, b, c, d\} \\ 1 & \mapsto a \\ 2 & \mapsto b \\ 3 & \mapsto a \\ 4 & \mapsto d \end{array} \right.$$

Si on choisit  $A = \{1, 2\}$  et  $A' = \{2, 3\}$ .

Alors,  $u(A) = \{a, b\}$ , et  $u(A') = \{a, b\}$  et  $u(A \cap A') = u(\{2\}) = \{b\}$

et  $u(A) \cap u(A') = \{a, b\} \not\subset \{b\}$  □

## 2.6 Montrer que, si $u$ est une application de $E$ dans $F$ . Si $B$ est une partie de $F$ , alors $u^{-1}(F \setminus B) = E \setminus u^{-1}(B)$ .

*Démonstration.* Soit  $x \in u^{-1}(F \setminus B)$ . Raisonnons par équivalences.

$$\begin{aligned} x \in u^{-1}(F \setminus B) &\iff u(x) \in F \setminus B \\ &\iff \text{non}(u(x) \in B) \\ &\iff \text{non}(x \in u^{-1}(B)) \\ &\iff x \in E \setminus u^{-1}(B) \end{aligned}$$

□

## 2.7 Montrer que, parmi les entiers ne s'écrivant qu'avec des 7, il existe au moins un multiple de 61.

*Démonstration.* Posons  $s$  la suite des entiers tels que  $\forall n \in \mathbb{N}^*, s_n = \underbrace{7 \dots 7}_{n \text{ fois}}$ . Considérons les 62 premiers termes de la suite.

Puisqu'il y a 61 classes de congruences modulo 61, le principe des tiroirs de Dirichlet nous permet d'affirmer que  $\exists (k, l) \in \llbracket 1, 62 \rrbracket^2, k < l : s_k \equiv s_l [61]$ .

Remarquons maintenant que  $s_l - s_k \equiv 0 [61]$ , autrement dit que  $61 \mid s_l - s_k$ .

Cependant,

$$s_l - s_k = \underbrace{7 \dots 7}_{l \text{ fois}} - \underbrace{7 \dots 7}_{k \text{ fois}} = \underbrace{7 \dots 7}_{l-k \text{ fois}} \underbrace{0 \dots 0}_{k \text{ fois}} = s_{l-k} \times 10^k$$

Donc  $61 \mid 10^k \times s_{l-k}$ , mais  $\text{pgcd}(61, 10^k) = 1$  donc le théorème de Gauss donne  $61 \mid s_{l-k}$ .

Ainsi, parmi les entiers ne s'écrivant qu'avec des 7, il existe au moins un multiple de 61.  $\square$

### 3 Semaine 3

#### 3.1 Preuve de l'inégalité triangulaire et de l'inégalité montrant que le module est 1-lipschitzien + dessin et interprétation géométrique

Pour tout  $(z_1, z_2) \in \mathbb{C}^2$ ,

- (i)  $|z_1 + z_2| \leq |z_1| + |z_2|$
- (ii)  $\left| |z_1| - |z_2| \right| \leq |z_1 - z_2|$

*Démonstration.* Soient  $(z_1, z_2) \in \mathbb{C}^2$  fixés quelconques.

◇ Si  $z_2 = 0$  l'inégalité est évidente Sinon,  $z_2 \neq 0$  alors  $|z_1 + z_2| \leq |z_1| + |z_2| \iff \left| 1 + \frac{z_1}{z_2} \right| \leq 1 + \left| \frac{z_1}{z_2} \right|$ . Posons  $u = \frac{z_1}{z_2}$

$$\begin{aligned} |1+u|^2 - (1+|u|)^2 &= (1+u)(\overline{1+u}) - (1+2|u|+|u|^2) \\ &= (1+u)(1+\bar{u}) - 1 - 2|u| - |u|^2 \\ &= u + \bar{u} - 2|u| \\ &= 2(\operatorname{Re}(u) - |u|) \leq 0 \end{aligned}$$

◇ Appliquons l'inégalité triangulaire

$$|z_1| = |z_1 - z_2 + z_2| \leq |z_1 - z_2| + |z_2| \implies |z_1| - |z_2| \leq |z_1 - z_2|$$

Puisque  $z_1$  et  $z_2$  jouent de rôles symétriques on a aussi

$$|z_2| - |z_1| \leq |z_2 - z_1| = |z_1 - z_2|$$

Donc

$$\left| |z_1| - |z_2| \right| \leq |z_1 - z_2|$$

□

#### 3.2 Caractérisation du cas d'égalité de l'inégalité triangulaire dans $\mathbb{C}$

*Démonstration.* ★ ( $\implies$ ) Supposons qu'il y ait égalité dans l'inégalité triangulaire

◇ Si  $z_2 = 0$  alors  $z_1$  et  $z_2$  sont positivement liés

◇ Sinon  $|1+u|^2 - (1+|u|)^2 = 0$  donc  $\operatorname{Re}(u) - |u| = 0$  Donc  $u \in \mathbb{R}_+$  mais  $z_1 = uz_2$ . Donc  $z_1$  et  $z_2$  sont positivement liés.

★ ( $\impliedby$ ) Supposons que  $z_1$  et  $z_2$  sont positivement liés. Alors il existe  $\lambda \in \mathbb{R}_+$  tel que  $z_1 = \lambda z_2$   
Si  $z_1 = \lambda z_2$

$$|z_1 + z_2| = |(\lambda + 1)z_2| = |\lambda + 1||z_2| = (\lambda + 1)|z_2| = \lambda|z_2| + |z_2| = |\lambda z_2| + |z_2| = |z_1| + |z_2|$$

Donc l'inégalité est une égalité

Si  $z_2 = \lambda z_1$ , en échangeant les rôles joués par  $z_1$  et  $z_2$  on obtient que l'inégalité est une égalité.

□

#### 3.3 Calcul de $\sum_{k=0}^n \cos(k\theta)$ pour tout $\theta \in \mathbb{R}$

*Démonstration.* Soit  $\theta \in \mathbb{R}$  fixé quelconque,  $n \in \mathbb{N}$  fixé quelconque.

$$\begin{aligned} C_n(\theta) &= \sum_{k=0}^n \cos(k\theta) = \sum_{k=0}^n \operatorname{Re}(e^{ik\theta}) \\ &= \operatorname{Re} \left( \sum_{k=0}^n e^{ik\theta} \right) \\ &= \operatorname{Re} \left( \sum_{k=0}^n (e^{i\theta})^k \right) \text{ par les formules de moivre} \end{aligned}$$



Ainsi, si  $e^{i\theta} = 1 \iff \theta \equiv 0[2\pi]$ ,

$$C_n(\theta) = \operatorname{Re} \left( \sum_{k=0}^n (1)^k \right) = \operatorname{Re}(n+1) = n+1$$

Sinon,

$$C_n(\theta) = \operatorname{Re} \left( \frac{1 - (e^{i\theta})^{n+1}}{1 - e^{i\theta}} \right)$$

Simplifions donc ce quotient.

$$\begin{aligned} \frac{1 - (e^{i\theta})^{n+1}}{1 - e^{i\theta}} &= \frac{1 - e^{i\theta(n+1)}}{1 - e^{i\theta}} = \frac{e^{\frac{i\theta(n+1)}{2}} \left( e^{-\frac{i\theta(n+1)}{2}} - e^{\frac{i\theta(n+1)}{2}} \right)}{e^{i\frac{\theta}{2}} \left( e^{-i\frac{\theta}{2}} - e^{i\frac{\theta}{2}} \right)} \\ &= e^{i\frac{\theta n}{2}} \left( \frac{-2i \sin\left(\frac{\theta(n+1)}{2}\right)}{-2i \sin\frac{\theta}{2}} \right) \\ &= \frac{\sin\left(\frac{\theta(n+1)}{2}\right)}{\sin\frac{\theta}{2}} \left( \cos\frac{\theta n}{2} + i \sin\frac{\theta n}{2} \right) \quad (\clubsuit) \end{aligned}$$

En prenant la partie réelle de ce résultat, on a

$$C_n(\theta) = \operatorname{Re} \left[ \frac{\sin\left(\frac{\theta(n+1)}{2}\right)}{\sin\frac{\theta}{2}} \left( \cos\frac{\theta n}{2} + i \sin\frac{\theta n}{2} \right) \right] = \frac{\sin\left(\frac{\theta(n+1)}{2}\right)}{\sin\frac{\theta}{2}} \cos\frac{n\theta}{2}$$

Donc

$$C_n(\theta) = \begin{cases} n+1 & \text{si } \theta \equiv 0[2\pi] \\ \frac{\sin\left(\frac{\theta(n+1)}{2}\right)}{\sin\frac{\theta}{2}} \cos\frac{n\theta}{2} & \text{sinon} \end{cases}$$

□

**Remarque** En prenant la partie imaginaire de  $(\clubsuit)$ , on peut retrouver la somme  $S_n(\theta)$  :

$$S_n(\theta) = \sum_{k=0}^n \sin(k\theta) = \begin{cases} 0 & \text{si } \theta \equiv 0[2\pi] \\ \frac{\sin\left(\frac{\theta(n+1)}{2}\right)}{\sin\frac{\theta}{2}} \sin\frac{n\theta}{2} & \text{sinon} \end{cases}$$

### 3.4 Si $z_0$ est racine de la fonction polynômiale $P$ , alors $P$ se factorise par $(z - z_0)$

Soient  $n \in \mathbb{N}$ ,  $(a_0, \dots, a_n) \in \mathbb{C}^{n+1}$  et  $z_0 \in \mathbb{C}$  Posons pour tout  $z \in \mathbb{C}$ ,  $P(z) = \sum_{k=0}^n a_k z^k$

(i) Si  $P(z_0) = 0$ , alors  $\exists Q \in \mathbb{C}[z] : \forall z \in \mathbb{C}, P(z) = (z - z_0)Q(z)$

*Démonstration.* Soit  $z \in \mathbb{C}$  fixé quelconque,

$$\begin{aligned} P(z) &= P(z) - P(z_0) \\ &= \sum_{k=0}^n a_k z^k - \sum_{k=0}^n a_k z_0^k \\ &= \sum_{k=0}^n a_k (z^k - z_0^k) \quad \text{nul pour } k=0 \\ &= \sum_{k=1}^n \left( a_k (z - z_0) \left( \sum_{j=0}^{k-1} z^j z_0^{k-1-j} \right) \right) \\ &= (z - z_0) \sum_{k=1}^n a_k \left( \sum_{j=0}^{k-1} z^j z_0^{k-1-j} \right) \end{aligned}$$

Donc en posant  $Q(z) = \sum_{k=1}^n a_k \left( \sum_{j=0}^{k-1} z^j z_0^{k-1-j} \right) \in \mathbb{C}[z]$ , on a montré que  $P$  se factorise.

□

### 3.5 Si $z_1, \dots, z_n$ sont $n$ racines distinctes de la fonction polynômiale $P$ de degré $n$ , alors $P(z)$ se factorise en ...

Soient  $n \in \mathbb{N}$ ,  $(a_0, \dots, a_n) \in \mathbb{C}^{n+1}$  et  $z_0 \in \mathbb{C}$  Posons pour tout  $z \in \mathbb{C}$ ,  $P(z) = \sum_{k=0}^n a_k z^k$

(ii) Si  $\exists p \in \mathbb{N}^* : \exists (z_1, \dots, z_p) \in \mathbb{C}^p$  deux à deux distincts tels que  $\forall k \in \llbracket 1, p \rrbracket, P(z_k) = 0$  alors,  $\exists Q \in \mathbb{C}[z] : \forall z \in \mathbb{C}, P(z) = Q(z) \times \prod_{k=1}^p (z - z_k)$ .

*Démonstration.* Considérons la propriété  $\mathcal{P}(\cdot)$  définie pour tout  $p \in \mathbb{N}^*$  par

$$\mathcal{P}(p) : \forall P \in \mathbb{C}[z], (\exists (z_1, \dots, z_p) \in \mathbb{C}^p, 2 \text{ à } 2 \text{ distincts} : \forall i \in \llbracket 1, p \rrbracket, P(z_i) = 0) \implies \exists Q \in \mathbb{C}[z] : P(z) = Q(z) \prod_{i=1}^p (z - z_i)$$

◇  $\mathcal{P}(1)$  est vraie d'après la preuve précédente.

◇ Soit  $p \in \mathbb{N}^*$  fixé quelconque tel que  $\mathcal{P}(p)$  est vraie. Soit  $P \in \mathbb{C}[z]$  tq  $\exists (z_1, \dots, z_{p+1}) \in \mathbb{C}^{p+1}$  deux à deux distincts tels que  $\forall i \in \llbracket 1, p+1 \rrbracket, P(z_i) = 0$ . Appliquons  $\mathcal{P}(p)$  à  $P \in \mathbb{C}[z]$  dont  $(z_1, \dots, z_p)$  sont les  $p$  racines deux à deux distinctes.

$$\exists Q_1 \in \mathbb{C}[z] : \forall z \in \mathbb{C}, P(z) = Q_1(z) \prod_{i=1}^p (z - z_i)$$

Évaluons cette expression en  $z_{p+1}$

$$\underbrace{P(z_{p+1})}_{=0} = Q_1(z_{p+1}) \prod_{i=1}^p \underbrace{(z_{p+1} - z_i)}_{\neq 0 \text{ car distincts}}$$

Donc  $Q_1(z_{p+1}) = 0$ , ce qui permet d'appliquer (i) pour  $P \leftarrow Q_1$ ,  $z_0 \leftarrow z_{p+1}$ .

$$\exists Q \in \mathbb{C}[z] : \forall z \in \mathbb{C}, Q_1(z) = (z - z_{p+1})Q(z)$$

Donc

$$\forall z \in \mathbb{C}, P(z) = (z - z_{p+1})Q(z) \prod_{i=1}^p (z - z_i) = Q(z) \prod_{i=1}^{p+1} (z - z_i)$$

Donc  $\mathcal{P}(p+1)$  est vraie. □

### 3.6 Calculer le module et un argument de $z = 1 + e^{i\theta}$ en fonction de $\theta \in [0, 2\pi[$

*Démonstration.* Soit  $\theta \in [0, 2\pi[$

$$z = 1 + e^{i\theta} = e^{i \times 0} + e^{i\theta} = e^{i \frac{\theta}{2}} \left( e^{-i \frac{\theta}{2}} + e^{i \frac{\theta}{2}} \right) = 2 \cos \frac{\theta}{2} e^{i \frac{\theta}{2}}$$

Cette dernière notation est une notation exponentielle seulement si  $2 \cos \frac{\theta}{2} \geq 0$ .

★ Si  $\theta \in [0, \pi[$ ,

$$\begin{cases} |z| = 2 \cos \frac{\theta}{2} \\ \frac{\theta}{2} \in \text{Arg}(z) \end{cases}$$

★ Si  $\theta = \pi$ ,  $z = 0$  donc  $|z| = 0$

★ Si  $\theta \in ]\pi, 2\pi[$ ,

$$\begin{aligned} z &= 2 \cos \frac{\theta}{2} e^{i \frac{\theta}{2}} = -2 \left| \cos \frac{\theta}{2} \right| e^{i \frac{\theta}{2}} \\ &= -2 \left| \cos \frac{\theta}{2} \right| e^{i(\frac{\theta}{2} + \pi)} \end{aligned}$$

Donc

$$\begin{cases} |z| = -2 \left| \cos \frac{\theta}{2} \right| \\ \frac{\theta}{2} + \pi \in \text{Arg}(z) \end{cases}$$

□

### 3.7 Décrire (avec preuve) l'ensemble des racines $n$ -ièmes de l'unité et les localiser géométriquement dans le plan complexe.

Pour tout  $n \in \mathbb{N}^* \setminus \{1\}$ ,

$$\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}} \mid k \in \llbracket 0, n-1 \rrbracket \right\}$$

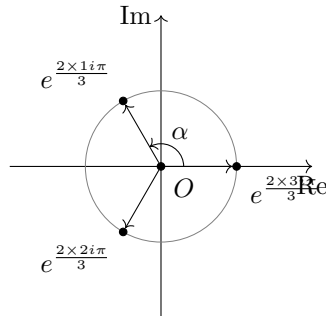
*Démonstration.* — Description de l'ensemble  $\mathbb{U}_n$

$$\begin{aligned} \left\{ \begin{array}{l} z^n = 1 \\ z \in \mathbb{C} \end{array} \right\} &\iff \left\{ \begin{array}{l} z^n = 1 \\ z \in \mathbb{C}^* \end{array} \right\} \text{ ou } \left\{ \begin{array}{l} z^n = 1 \\ z = 0 \end{array} \right\} \\ &\iff \left\{ \begin{array}{l} \rho^n e^{in\theta} = 1 \\ z = \rho e^{i\theta} \\ (\rho, \theta) \in \mathbb{R}_+^* \times \mathbb{R} \end{array} \right\} \\ &\iff \left\{ \begin{array}{l} \rho^n = 1 \\ n\theta \equiv 0[2\pi] \\ z = \rho e^{i\theta} \\ (\rho, \theta) \in \mathbb{R}_+^* \times \mathbb{R} \end{array} \right\} \\ &\iff \left\{ \begin{array}{l} \rho = 1 \text{ car } \rho > 0 \\ \theta \equiv 0 \left[ \frac{2\pi}{n} \right] \\ z = \rho e^{i\theta} \\ (\rho, \theta) \in \mathbb{R}_+^* \times \mathbb{R} \end{array} \right\} \\ &\iff \left\{ \begin{array}{l} \rho = 1 \\ \exists k \in \mathbb{Z} : \theta = \frac{2k\pi}{n} \\ z = \rho e^{i\theta} \\ (\rho, \theta) \in \mathbb{R}_+^* \times \mathbb{R} \end{array} \right\} \\ &\iff \exists k \in \mathbb{Z} : z = e^{\frac{2ik\pi}{n}} \\ &\iff z \in \left\{ e^{\frac{2ik\pi}{n}} \mid k \in \mathbb{Z} \right\} \end{aligned}$$

L'ensemble des solutions est paramétré par l'entier  $k$  qui parcourt un ensemble infini. Toutefois, en représentant graphiquement les solutions, il semblerait que "tous les  $n$ ", on fait un tour de cercle trigonométrique de plus, en redécrivant les solutions déjà obtenues pour  $k \in \llbracket 0, n-1 \rrbracket$ .

— Localisation géométrique

- ★  $\mathbb{U}_3$  est l'ensemble des sommets du triangle équilatéral inscrit dans le cercle unité, et dont 1 est l'un des sommets

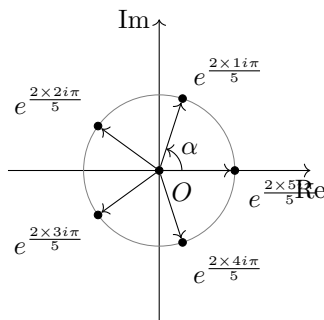


- ★  $\mathbb{U}_4$  est l'ensemble des sommets du carré inscrit dans le cercle unité et dont 1 est l'un des sommets. Le côté du carré vaut  $|1 - i| = \sqrt{2}$ .
- ★  $\mathbb{U}_5$  est l'ensemble des sommets du pentagone régulier inscrit dans le cercle unité et dont 1 est l'un des sommets.

□

### 3.8 Somme et Produit des racines $n$ -ièmes

*Démonstration.* ◇ **Méthode 1** En utilisant les relations coefficients racines.



$\mathbb{U}_n$  sont les  $n$  racines distinctes de  $z^n - 1$

$$S_n = -\frac{1}{\text{coefficient dominant}} \times (\text{coefficient de } z^{n-1} \text{ dans } z^n - 1) = \begin{cases} -0 & \text{si } n \geq 2 \\ -(-1) & \text{sinon} \end{cases}$$

$$P_n = (-1)^n \frac{\text{coefficient constant}}{\text{coefficient dominant}} = (-1)^n \times \frac{-1}{1} = (-1)^{n+1}$$

◇ **Méthode 2** Manipulation des symboles sommatoires

$$\begin{aligned} S_n &= \sum_{\omega \in \mathbb{U}_n} \omega = \sum_{k=0}^{n-1} \omega_0^k \\ &= \begin{cases} 1 & \text{si } n = 1 \\ 1 \times \frac{1-\omega_0^n}{1-\omega_0} & \text{sinon} \end{cases} \end{aligned}$$

Puisqu'on ne peut appliquer la formule de la somme des termes d'une suite géométrique seulement si la raison  $\omega_0 = 1 \iff e^{\frac{2i\pi}{n}} = 1 \iff \frac{2\pi}{n} \equiv 0[2\pi] \iff n = 1$

De même

$$P_n = \prod_{\omega \in \mathbb{U}_n} \omega = \prod_{k=0}^{n-1} \omega_0^k = \omega_0^{\sum_{k=0}^{n-1} k} = \omega_0^{\frac{n(n-1)}{2}}$$

$$\begin{aligned} &= \begin{cases} (\omega_0^n)^{\frac{n-1}{2}} = 1^{\frac{n-1}{2}} = 1 & \text{si } n \equiv 1[2] \\ e^{\frac{2i\pi n(n-1)}{2n}} = e^{i\pi(n-1)} = (-1)^{n-1} & \end{cases} \\ &= (-1)^{n-1} \end{aligned}$$

□

## 4 Semaine 4

### 4.1 Résolution des équations algébriques de degré 2 dans $\mathbb{C}$ et algorithme de recherche d'une racine carrée sous forme cartésienne (sur un exemple explicite).

Considérons l'équation algébrique de degré 2 :

$$az^2 + bz + c = 0$$

Où  $z \in L$  est l'inconnue et  $(a, b, c) \in \mathbb{C}^* \times \mathbb{C}^2$  sont des paramètres. Posons  $\Delta = b^2 - 4ac$  que l'on appelle le discriminant de l'équation.

- Si  $\Delta = 0$ , l'équation admet une unique solution dite double qui est  $-\frac{b}{2a}$  et la forme factorisée du trinôme est

$$az^2 + bz + c = a \left( z + \frac{b}{2a} \right)^2$$

- Si  $\Delta \neq 0$ , notons  $\delta$  une racine carrée de  $\Delta$ , l'équation admet deux solutions distinctes  $\frac{-b-\delta}{2a}$  et  $\frac{-b+\delta}{2a}$  dites simples et la forme factorisée du trinôme est

$$az^2 + bz + c = a \left( z - \frac{-b-\delta}{2a} \right) \left( z - \frac{-b+\delta}{2a} \right)$$

*Démonstration.* La preuve est immédiate à partir de la forme canonique du trinôme du second degré :

La preuve est immédiate à partir de la forme canonique du trinôme du second degré :

$$\begin{aligned} az^2 + bz + c &= a \left[ \underbrace{z^2 + \frac{b}{a}z}_{\text{But : Absorber ces termes dans un carré}} + \frac{c}{a} \right] = a \left[ z^2 + 2\frac{b}{2a}z + \frac{b^2}{4a^2} - \frac{b^2}{4a^2} + \frac{c}{a} \right] \\ &= a \left[ \left( z + \frac{b}{2a} \right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} \right] \\ &= a \left[ \left( z + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right] \\ &= a \left[ \left( z + \frac{b}{2a} \right)^2 - \frac{\Delta}{4a^2} \right] \end{aligned}$$

- Si  $\Delta = 0$

$$az^2 + bz + c = a \left( z - \frac{-b}{2a} \right)^2$$

de sorte que

$$az^2 + bz + c = 0 \iff a \left( z - \frac{-b}{2a} \right)^2 = 0 \iff z = -\frac{b}{2a}$$

- Sinon

$$\begin{aligned} az^2 + bz + c &= a \left[ \left( z + \frac{b}{2a} \right)^2 - \left( \frac{\delta}{2a} \right)^2 \right] = a \left( z + \frac{b}{2a} - \frac{\delta}{2a} \right) \left( z + \frac{b}{2a} + \frac{\delta}{2a} \right) \\ &= a \left( z - \frac{-b+\delta}{2a} \right) \left( z - \frac{-b-\delta}{2a} \right) \end{aligned}$$

de sorte que

$$az^2 + bz + c = 0 \iff a \left( z - \frac{-z + \delta}{2a} \right) \left( z - \frac{-z - \delta}{2a} \right) = 0$$

$$\iff \begin{cases} z - \frac{-z - \delta}{2a} = 0 \\ \text{ou} \\ z - \frac{-z + \delta}{2a} = 0 \end{cases}$$

$$\iff \begin{cases} z = \frac{-z - \delta}{2a} \\ \text{ou} \\ z = \frac{-z + \delta}{2a} \end{cases}$$

□

## 4.2 Résolution de $e^z = z_0$ où $z_0 \in \mathbb{C}^*$

L'exponentielle complexe a pour image  $\mathbb{C}^*$  et, pour tout  $z_0 \in \mathbb{C}^*$ ,

$$\exp_{\mathbb{C}}^{-1}(\{z_0\}) = \{\ln|z_0| + i\theta_0 + 2ik\pi \mid k \in \mathbb{Z}\}$$

où  $\theta_0 \in \arg(z_0)$

*Démonstration.* La propriété, pour tout  $z \in \mathbb{C}$ ,  $|e^z| = |e^{\operatorname{Re}(z)}| > 0$  montre que  $0 \notin \exp_{\mathbb{C}}(\mathbb{C})$ .  
 $z_0 \neq 0$  donc  $\exists \theta_0 \in \arg(z_0) : z_0 = |z_0|e^{i\theta_0}$ . Résolvons l'équation d'inconnue  $z \in \mathbb{C}$

$$\exp_{\mathbb{C}}(z) = z_0 \iff e^{\operatorname{Re}(z)} e^{i\operatorname{Im}(z)} = |z_0|e^{i\theta_0}$$

$$\iff \begin{cases} e^{\operatorname{Re}(z)} = |z_0| \\ \text{et} \\ \operatorname{Im}(z) \equiv \theta_0[2\pi] \end{cases}$$

$$\iff \begin{cases} \operatorname{Re}(z) = \ln|z_0| \\ \text{et} \\ \operatorname{Im}(z) \equiv \theta_0[2\pi] \end{cases}$$

$$\iff z \in \{\ln|z_0| + i\theta_0 + 2ik\pi \mid k \in \mathbb{Z}\}$$

□

## 4.3 Montrer l'unicité de l'élément neutre et du symétrique d'un élément sous des hypothèses sur la loi à préciser.

*Démonstration.* ◇ Unicité de l'élément neutre bilatère

Soient  $(e_1, e_2) \in E^2$  fixés quelconques tels que  $\begin{cases} \forall x \in E, x * e_1 = e_1 * x = x \\ \forall x \in E, x * e_2 = e_2 * x = x \end{cases}$  Particularisons la première relation pour  $x \leftarrow e_2$  :

$$e_2 * e_1 = e_1 * e_2 = e_2$$

En particulierisant, de même la deuxième relation pour  $x \leftarrow e_1$

$$e_1 * e_2 = e_2 * e_1 = e_2$$

D'où, par transitivité de l'égalité :  $e_1 = e_2$

◇ Unicité du symétrique sous réserve d'existence (LCI associative d'unité  $e$ ) Soit  $a \in E$  symétrisable

$$\exists z \in E : a * z = z * a = e$$

Fixons un tel  $z$  pour la suite de la preuve

— L'ensemble  $\{y \in E \mid a * y = y * a = e\}$  n'est pas vide puisqu'il contient  $z$ .

— Soit  $b \in \{y \in E \mid a * y = y * a = e\}$  fixé quelconque. Alors

$$\begin{aligned} a * b = e &\implies z * (a * b) = z * e \\ &\implies \underbrace{z * a}_e * b = z * e \text{ par associativité} \\ &\implies b = z \end{aligned}$$

Donc l'ensemble  $\{y \in E \mid a * y = y * a = e\}$  contient au plus un élément neutre, qui est  $z$ .  $\square$

#### 4.4 Preuve de la caractérisation d'un sous-groupe, application au fait que $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$ .

Soit  $(G, *)$  un groupe, et  $H$  une partie de  $G$

$$H \text{ est un sous groupe de } G \iff \begin{cases} H \neq \emptyset \\ \forall (x, y) \in H^2, x * y^{-1} \in H \end{cases}$$

*Démonstration.*  $\star$  Supposons que  $H$  est un sous groupe de  $G$  Par définition d'un sous groupe,  $H \neq \emptyset$ .

Soient  $(x, y) \in H^2$  fixés quelconques  $H$  est un sous groupe, donc  $y$  est symétrisable dans  $H$  :  $y^{-1} \in H$  De plus, c'est un groupe, donc stable pour la loi  $*$ , donc  $x * y^{-1} \in H$

$$\star \text{ Supposons que } \begin{cases} H \neq \emptyset & (1) \\ \forall (x, y) \in H^2, x * y^{-1} \in H & (2) \end{cases}$$

$\diamond$   $H$  est non vide par hypothèse

$\diamond$  Puisque  $H \neq \emptyset$ ,  $\exists x \in H$  Ainsi,  $x * x^{-1} \in H$  donc  $e \in H$

$\diamond$  Soient  $(x, y) \in H^2$  fixés quelconques.  $y \in H$  permet d'appliquer (2) pour  $x \leftarrow y$  et  $y \leftarrow e$  :

$$e * y^{-1} \in H$$

Donc  $y^{-1} \in H$ . Tout élément est symétrisable dans  $H$

$\diamond$  Soient  $(x, y) \in H^2$  fixés quelconques. On a montré que  $y$  est symétrisable dans  $H$ , donc en appliquant (2) pour  $x \leftarrow x$  et  $y \leftarrow y^{-1}$  :

$$x * (y^{-1})^{-1} \in H \implies x * y \in H$$

Donc  $H$  est stable pour la loi  $H$ .

Donc  $H$  est un sous groupe de  $G$ .  $\square$

#### Application aux racines n-ièmes de l'unité

Soit  $n \in \mathbb{N}^*$  fixé quelconque

$\star \forall z \in \mathbb{U}_n, z^n = 1$  donc  $1 = |z^n| = |z|^n$ . Or  $|z| \geq 0$  donc  $|z| = 1$ , si bien que  $\mathbb{U}_n \subset \mathbb{U}$

$\star \mathbb{U}_n \neq \emptyset$  car  $1 \in \mathbb{U}_n$

$\star$  Soient  $(z_1, z_2) \in \mathbb{U}_n$  fixés quelconques. Calculons

$$(z_1 z_2^{-1})^n = \left( \frac{z_1}{z_2} \right)^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1$$

Donc  $z_1 z_2^{-1} \in \mathbb{U}_n$ . On a donc montré que  $(\mathbb{U}_n, \times)$  est un sous groupe de  $(\mathbb{U}, \times)$ .

#### 4.5 Si $\varphi$ est un morphisme de groupes de $G_1$ de neutre $e_1$ dans $G_2$ de neutre $e_2$ , calculer $\varphi(e_1)$ et $\varphi(x^{-1})$

*Démonstration.*  $\star$  Soit  $f$  un morphisme de groupe de  $(G_1, *_1)$  dans  $(G_2, *_2)$

D'une part  $f(e_1 *_1 e_1) = f(e_1)$  D'autre part, par propriété de morphisme,  $f(e_1 *_1 e_1) = f(e_1) *_2 f(e_1)$  Donc

$$f(e_1) *_2 f(e_1) = f(e_1)$$

Si l'on compose à gauche par  $f(e_1)^{-1}$

$$\begin{aligned} f(e_1)^{-1} *_2 f(e_1) *_2 f(e_1) &= f(e_1)^{-1} *_2 f(e_1) \\ \implies f(e_1) &= e_2 \end{aligned}$$

★ Soit  $x \in G_1$  fixé quelconque

$$f(x) *_2 f(x^{-1}) = f(x *_1 x^{-1}) = f(e_1) = e_2$$

Composons les deux membres à gauche par  $f(x)^{-1}$

$$f(x)^{-1} *_2 f(x) *_2 f(x^{-1}) = f(x)^{-1} *_2 e_2$$

Donc

$$f(x^{-1}) = f(x)^{-1}$$

□

#### 4.6 Montrer que l'image d'un sous-groupe par un morphisme de groupes est un sous-groupe du groupe d'arrivée

*Démonstration.* Soit  $f$  un morphisme de groupe de  $(G_1, *_1)$  dans  $(G_2, *_2)$ . Notons  $e_1$  et  $e_2$  les neutres respectifs de  $G_1$  et  $G_2$ .

Soit  $H_1$  un sous groupe de  $G_1$  fixé quelconque

★  $f(H_1)$  est par définition une partie de  $G_2$

★  $f(H_1) \neq \emptyset$  car  $H_1$  est un groupe, qui contient  $e_1$   $f(e_1) = e_2$  donc  $e_2 \in f(H_1)$

★ Soient  $(g_2, h_2) \in f(H_1)^2$  fixés quelconques alors  $\exists (g_1, h_1) \in H_1 : f(g_1) = g_2, f(h_1) = h_2$  donc

$$g_2 *_2 h_2^{-1} = f(g_1) *_2 f(h_1^{-1}) = f\left(\underbrace{g_1 *_1 h_1^{-1}}_{\in H_1 \text{ car sous groupe de } G_1}\right)$$

Donc  $g_2 *_2 h_2^{-1} \in f(H_1)$  Donc  $f(H_1)$  est un sous groupe de  $G_2$

□

#### 4.7 Montrer que l'image réciproque par un morphisme de groupes d'un sous-groupe est toujours un sous-groupe du groupe de départ,

*Démonstration.* Soit  $f$  un morphisme de groupe de  $(G_1, *_1)$  dans  $(G_2, *_2)$ . Notons  $e_1$  et  $e_2$  les neutres respectifs de  $G_1$  et  $G_2$ .

Soit  $H_2$  un sous groupe de  $G_2$  fixé quelconque

★  $f^{-1}(H_2)$  est par définition une partie de  $G_1$

★  $f^{-1}(H_2) \neq \emptyset$  car  $H_2$  est un groupe, qui contient  $e_2$   $f(e_1) = e_2$  donc  $e_1 \in f^{-1}(H_2)$

★ Soient  $(g_1, h_1) \in f^{-1}(H_2)^2$  fixés quelconques alors  $f(g_1) \in H_2$  et  $f(h_1) \in H_2$  donc

$$f(g_1 *_1 h_1^{-1}) = \underbrace{f(g_1)}_{\in H_2} *_2 \underbrace{f(h_1^{-1})}_{\in H_2} \in H_2 \text{ car c'est un sous groupe}$$

Donc  $f(g_1 *_1 h_1^{-1}) \in H_2$  donc  $g_1 *_1 h_1^{-1} \in f^{-1}(H_2)$

Donc  $f^{-1}(H_2)$  est un sous groupe de  $G_1$

□

**Application 1 :** Le noyau d'un morphisme est un sous-groupe

Le noyau, noté  $\ker f$  est par définition égal à  $f^{-1}(\{e_2\})$  c'est donc un sous groupe de  $G_1$

**Application 2 :** Pour tout  $n \in \mathbb{N}$ ,  $\phi_n \left| \begin{array}{ccc} (\mathbb{C}^*, \times) & \rightarrow & (\mathbb{C}^*, \times) \\ z & \mapsto & z^n \end{array} \right.$  est un morphisme de groupes.

Son noyau,  $\ker \phi_n = \{z \in \mathbb{C}^* | z^n = 1\} = \mathbb{U}_n$ . D'après l'application 1,  $\ker \phi_n$  est un sous groupe de  $(\mathbb{C}^*, \times)$ . Donc  $(\mathbb{U}_n, \times)$  est un sous groupe de  $(\mathbb{C}^*, \times)$ .



## 5 Semaine 5

## 6 Semaine 6

### 6.1 Montrer que si $f$ est impaire et bijective, alors $f^{-1}$ est aussi impaire. Donnez un/des exemples.

*Démonstration.* Soit  $f : I \rightarrow F$ , avec  $I, F$  deux parties non-vides de  $\mathbb{R}$ , une telle fonction et notons  $f^{-1}$  sa bijection réciproque. Si  $f$  est impaire sur  $I$ , alors pour tout  $x \in I$ ,  $-x \in I$ , ainsi  $I$  est centré en 0 et on a :

$$\forall x \in I, f(-x) = -f(x).$$

Ainsi, prenons  $y \in F$ , alors  $-y \in F$  par imparité et bijectivité de  $f$ . On a donc :

$$\begin{aligned} f^{-1}(-y) &= f^{-1}(-f(f^{-1}(y))) \\ &= f^{-1}(f(-f^{-1}(y))) \\ &= -f^{-1}(y). \end{aligned}$$

D'où l'imparité de  $f^{-1}$ .

Pour ce qui est de l'exemple, prenons notre fonction bijective impaire préférée, la fonction  $\sin$   $\left| \begin{smallmatrix} [-1,1] \\ [-\frac{\pi}{2}, \frac{\pi}{2}] \end{smallmatrix} \right|$  que l'on notera  $\widetilde{\sin}$ . Sa bijection réciproque est bien entendu  $\arcsin : [-1, 1] \rightarrow [-\frac{\pi}{2}, \frac{\pi}{2}]$ .

De la même manière que dans la démonstration du cas général, prenons  $y \in [-1, 1]$ , comme  $[-1, 1]$  est centré en 0,  $-y \in [-1, 1]$ , on a dès lors :

$$\begin{aligned} \arcsin(-y) &= \arcsin(-\widetilde{\sin}(\arcsin(y))) \\ &= \arcsin(\widetilde{\sin}(-\arcsin(y))) \\ &= -\arcsin(y). \end{aligned}$$

□

### 6.2 Limite (et preuve) lorsque $x$ tend vers $+\infty$ de $\frac{(\ln x)^\alpha}{x^\beta}$ pour $\alpha, \beta \in (\mathbb{R}_+^*)^2$ .

*Démonstration.* Premièrement, posons :

$$\forall (x, \alpha, \beta) \in [1, +\infty[ \times (\mathbb{R}_+^*)^2, \quad f_{\alpha, \beta}(x) = \frac{(\ln x)^\alpha}{x^\beta}.$$

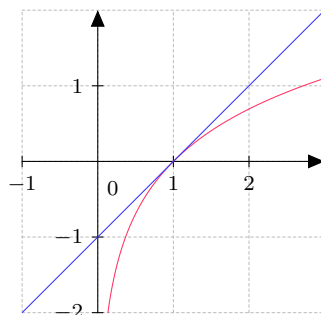
Deuxièmement, montrons que :

$$\frac{\ln(x)}{x^2} \xrightarrow{n \rightarrow +\infty} 0.$$

Soit  $x \in [1, +\infty[ = \mathcal{A}$ . Nous savons que la fonction  $\ln$  est concave sur  $\mathbb{R}_+^*$ , donc en particulier sur  $\mathcal{A}$ . Ainsi,  $\ln$  est en dessous de toutes ses tangentes, d'où :

$$\forall x \in \mathcal{A}, \quad 0 \leq \ln(x) \leq x - 1.$$

Illustration de l'inégalité :



**Figure 1.**  $\ln$  en rouge et la première bissectrice en bleu.

On peut alors diviser par  $x^2$  (car  $x \neq 0$ ) :

$$\forall x \in \mathcal{A}, \quad 0 \leq \underbrace{\frac{\ln(x)}{x^2}}_{f_{1,2}(x)} \leq \underbrace{\frac{1}{x}}_{\xrightarrow{x \rightarrow +\infty} 0} - \underbrace{\frac{1}{x^2}}_{\xrightarrow{x \rightarrow +\infty} 0}.$$

Donc par théorème d'encadrement  $f_{1,2}(x) \xrightarrow{x \rightarrow +\infty} 0$ .

Dernièrement, le cas général. Soit  $x \in \mathcal{A}$  et soient  $(\alpha, \beta) \in (\mathbb{R}_+^*)^2$ . On fait une preuve directe.

$$\begin{aligned} \frac{(\ln(x))^\alpha}{x^\beta} &= \left( \frac{\ln(x)}{x^{\frac{\beta}{\alpha}}} \right)^\alpha \\ &= \underbrace{\left( \frac{2\alpha}{\beta} \right)^\alpha}_{\substack{\text{c'te} \\ \text{(définie!)}}} \cdot \underbrace{\left[ \frac{\ln \left( x^{\frac{\beta}{2\alpha}} \right)}{\underbrace{\left( x^{\frac{\beta}{2\alpha}} \right)^2}_{\xrightarrow{x \rightarrow +\infty} 0}} \right]^\alpha}_{\substack{\text{d'après le dernier point} \\ \xrightarrow{x \rightarrow +\infty} 0}} \\ &\quad \underbrace{\xrightarrow{x \rightarrow +\infty} 0}_{\substack{\text{par composition des limites} \\ \text{par produit}}} \end{aligned}$$

□

**6.3 Limite en 0 de  $\frac{1-\cos(x)}{x^2}$  et limite en  $+\infty$  suivant  $n$  de  $\frac{(q^n)^\alpha}{(n!)^\beta}$  pour  $q \in \mathbb{R}$  et  $(\alpha, \beta) \in (\mathbb{R}_+^*)^2$ .**

*Démonstration.*

Montrons que  $\frac{1-\cos(x)}{x^2} \xrightarrow{x \rightarrow 0} \frac{1}{2}$ .

On fait toujours une preuve directe.

$$\begin{aligned}
\lim_{x \rightarrow 0} \frac{1 - \cos(x)}{x^2} &= \lim_{x \rightarrow 0} \frac{1 - \cos\left(\frac{2x}{2}\right)}{x^2} \\
&= \lim_{x \rightarrow 0} \frac{1 - \left(1 - 2 \sin^2\left(\frac{x}{2}\right)\right)}{x^2} \\
&= \lim_{x \rightarrow 0} \frac{2 \sin^2\left(\frac{x}{2}\right)}{4 \left(\frac{x}{2}\right)^2} \\
&= \lim_{x \rightarrow 0} \underbrace{\frac{1}{2}}_{\substack{\text{c'est} \\ \text{par produit}}} \cdot \underbrace{\left[ \frac{\sin\left(\frac{x}{2}\right)}{\left(\frac{x}{2}\right)} \right]^2}_{\substack{\xrightarrow{x \rightarrow 0} 1 \\ \text{limite usuelle} \\ \xrightarrow{x \rightarrow 0} 1 \\ \text{par composition}}} \\
&= \frac{1}{2}
\end{aligned}$$

Trouvons la limite, sous réserve d'existence, de  $\frac{(q^n)^\alpha}{(n!)^\beta}$  pour  $q \in \mathbb{R}$  et  $(\alpha, \beta) \in (\mathbb{R}_+^*)^2$  suivant  $n$  en  $+\infty$ .

Remarquons que si  $q \leq 0$ , il est **nécessaire** d'avoir  $\alpha \in \mathbb{Z}^*$  sinon l'expression n'a tout simplement **aucun sens**. De fait, on supposera  $q > 0$  tout le long, les cas  $q < 0$  se font naturellement (convergence pour  $q \in \mathbb{R}_-$ ).

Soit donc  $0 < q < 1$ , ce cas est immédiat,  $((q^n)^\alpha)_{n \in \mathbb{N}} = ((q^\alpha)^n)_{n \in \mathbb{N}}$ , donc il s'agit de la suite géométrique de raison  $q^\alpha \in ]0, 1[$  et de premier terme  $q^{\min_I(n)\alpha}$  ( $\min_I(n)$ , avec  $I$  une partie non vide de  $\mathbb{N}$ , car la suite ne démarre pas forcément à 0), donc elle converge vers 0.

Si  $q \geq 1$ , on montre le cas trivial  $\alpha = \beta = 1$  :

$$\forall n \in \llbracket [q] + 1, +\infty \llbracket, \quad 0 \leq \frac{q^n}{n!} = \underbrace{\frac{q}{1} \times \frac{q}{2} \times \cdots \times \frac{q}{[q]}}_{= \lambda \text{ (une constante)}} \times \underbrace{\frac{q}{[q] + 1}}_{\leq 1} \times \cdots \times \underbrace{\frac{q}{n-1}}_{\leq 1} \times \frac{q}{n} \leq \underbrace{\frac{\lambda q}{n}}_{\xrightarrow{n \rightarrow +\infty} 0}$$

Par théorème d'existence de limite par encadrement,  $\left(\frac{q^n}{n!}\right)_{n \in \mathbb{N}}$  converge et sa limite est 0.

Soient  $(\alpha, \beta) \in \mathbb{R}_+^*$ , montrons le cas général pour  $q \geq 1$ .

$$\forall n \in \mathbb{N}, \quad \frac{(q^n)^\alpha}{(n!)^\beta} = \left( \frac{\left(q^{\frac{\alpha}{\beta}}\right)^n}{n!} \right)^\beta = \underbrace{\left( \underbrace{\frac{\left(q^{\frac{\alpha}{\beta}}\right)^n}{n!}}_{\xrightarrow{n \rightarrow +\infty} 0} \right)^\beta}_{\substack{\xrightarrow{n \rightarrow +\infty} 0 \\ \text{par composition des limites } (\beta > 0)}}$$

□

## 6.4 Présentation exhaustive de la fonction arcsin.

*Démonstration.* Premièrement, ladite fonction est la bijection réciproque de la fonction  $\widetilde{\sin}$  (voir 1.). D'où :

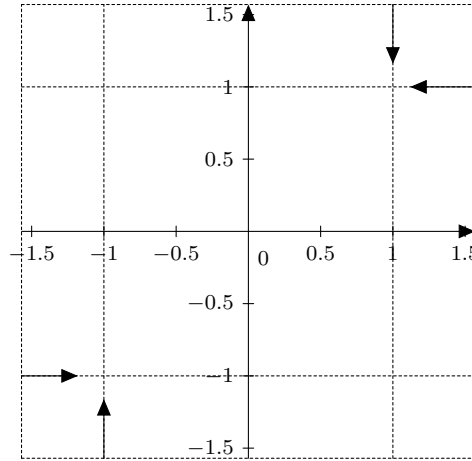
$$\arcsin = \begin{cases} [-1, 1] & \rightarrow [-\frac{\pi}{2}, \frac{\pi}{2}] \\ x & \mapsto (\widetilde{\sin})^{-1}(x) \end{cases}$$

Ainsi, pour  $x \in [-1, 1]$ ,  $\arcsin(x)$  est l'unique solution de l'équation d'inconnue  $\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ ,  $\sin(\theta) = x$ .

Il découle alors naturellement des propriétés héréditairement acquises de  $\widetilde{\sin}$  :

1. arcsin est impaire.
2. arcsin est strictement croissante sur  $[-1, 1]$ .
3.  $\arcsin \in \mathcal{C}^0([-1, 1], [-\frac{\pi}{2}, \frac{\pi}{2}])$ .
4.  $\arcsin \in \mathcal{D}^1(]-1, 1[, -\frac{\pi}{2}, \frac{\pi}{2}[)$ .
5.  $\arcsin'(x) = \frac{1}{\sqrt{1-x^2}}$  pour tout  $x \in ]-1, 1[$ .
6. arcsin admet deux demi-tangentes verticales en  $-1$  et  $1$ .

Graphes de arcsin :



**Figure 2.** arcsin en bleu,  $\widetilde{\sin}$  en vert et la première bissectrice en rouge.

On a aussi, grâce au taux d'accroissement en 0 d'arcsin :

$$\lim_{x \rightarrow 0} \frac{\arcsin(x)}{x} = 1.$$

Puis finalement (visible sur le graphe) :

$$\forall x \in [0, 1], \quad \arcsin(x) \geq x.$$

□

## 6.5 Présentation exhaustive de la fonction arccos.

*Démonstration.* Premièrement, ladite fonction est la bijection réciproque de la fonction  $\cos|_{[0, \pi]}^{[-1, 1]} := \widetilde{\cos}$ . D'où :

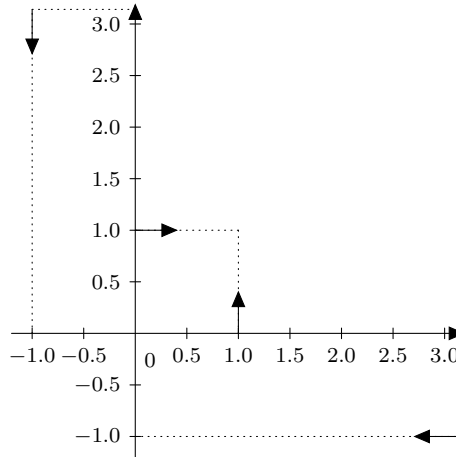
$$\arccos = \begin{cases} [-1, 1] & \rightarrow [0, \pi] \\ x & \mapsto (\widetilde{\cos})^{-1}(x) \end{cases}$$

Ainsi, pour  $x \in [-1, 1]$ ,  $\arccos(x)$  est l'unique solution de l'équation d'inconnue  $\theta \in [0, \pi]$ ,  $\cos(\theta) = x$ .

Il découle alors naturellement des propriétés héréditairement acquises de  $\widetilde{\cos}$  :

1.  $\arccos$  est strictement décroissante sur  $[-1, 1]$ .
2.  $\arccos \in \mathcal{C}^0([-1, 1], [0, \pi])$ .
3.  $\arccos \in \mathcal{D}^1(]-1, 1[, ]0, \pi[)$ .
4.  $\arccos'(x) = -\frac{1}{\sqrt{1-x^2}}$  pour tout  $x \in ]-1, 1[$ .
5.  $\arccos$  admet deux demi-tangentes verticales en  $-1$  et  $1$ .

Graphes de  $\arccos$  :



**Figure 3.**  $\arccos$  en vert,  $\widetilde{\cos}$  en violet, la première bissectrice en rouge et  $y = \frac{\pi}{2} - x$  en rose.

□

## 6.6 Présentation exhaustive de la fonction arctan.

*Démonstration.*

Premièrement, ladite fonction est la bijection réciproque de la fonction  $\tan|_{]-\frac{\pi}{2}, \frac{\pi}{2}[} := \widetilde{\tan}$ .  
D'où :

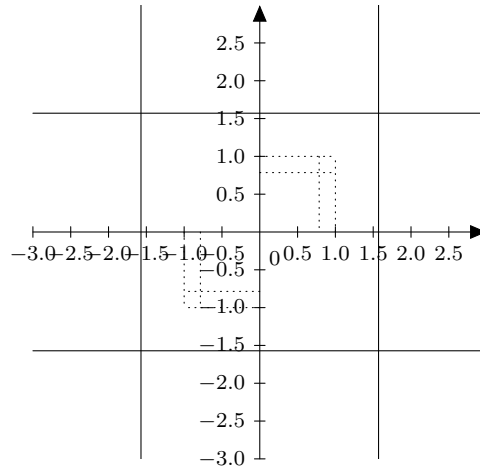
$$\arctan = \begin{cases} \mathbb{R} & \rightarrow & ]-\frac{\pi}{2}, \frac{\pi}{2}[ \\ x & \mapsto & (\widetilde{\tan})^{-1}(x) \end{cases}$$

Ainsi, pour  $x \in \mathbb{R}$ ,  $\arctan(x)$  est l'unique solution de l'équation d'inconnue  $\theta \in ]-\frac{\pi}{2}, \frac{\pi}{2}[$ ,  $\tan(\theta) = x$ .

Il découle alors naturellement des propriétés héréditairement acquises de  $\widetilde{\tan}$  :

1.  $\arctan$  est impaire.
2.  $\arctan \in \mathcal{C}^0(\mathbb{R}, ]-\frac{\pi}{2}, \frac{\pi}{2}[)$ .
3.  $\arctan \in \mathcal{D}^1(\mathbb{R}, ]-\frac{\pi}{2}, \frac{\pi}{2}[)$ .
4.  $\arctan'(x) = \frac{1}{1+x^2}$  pour tout  $x \in \mathbb{R}$ .

Graphe de arctan :



**Figure 4.** arctan en vert,  $\widetilde{\tan}$  en bleu, la première bissectrice en rouge, et les fonctions  $y = \pm \frac{\pi}{2}$  et  $x = \pm \frac{\pi}{2}$  en noir.

On a aussi (visible sur le graphe) :

$$\forall x \in \mathbb{R}_+, \quad \arctan(x) \leq x.$$

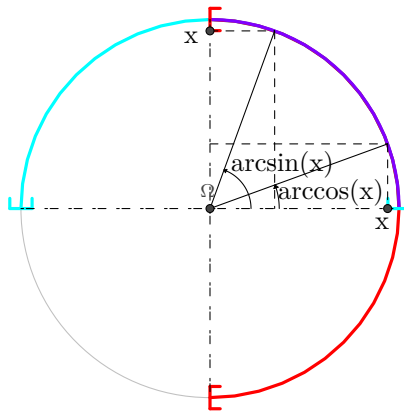
Et enfin :

$$\forall x \in \mathbb{R}^*, \quad \arctan(x) + \arctan\left(\frac{1}{x}\right) = \begin{cases} \frac{\pi}{2} & \text{si } x > 0 \\ -\frac{\pi}{2} & \text{si } x < 0. \end{cases}$$

□

## 6.7 2 preuves de $\arcsin(x) + \arccos(x) = \frac{\pi}{2}$ sur $[-1, 1]$ , dont une basée sur une interprétation géométrique du cercle trigonométrique.

*Démonstration.* L'interprétation géométrique sur  $[0, 1]$ , celle sur  $[-1, 0]$  est laissée au lecteur car il s'agit du même principe modulo des détails :



**Figure 5.**

Preuve formelle :

Soit  $x \in [-1, 1]$ . Posons  $\varphi = \arcsin(x) \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ . Ainsi :

$$\arcsin(x) + \arccos(x) = \varphi + \arccos(\sin(\varphi)) = \varphi + \arccos\left(\cos\left(\frac{\pi}{2} - \varphi\right)\right),$$

or  $\varphi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$  donc  $\frac{\pi}{2} - \varphi \in [0, \pi]$  d'où  $\arccos\left(\cos\left(\frac{\pi}{2} - \varphi\right)\right) = \frac{\pi}{2} - \varphi$  si bien que :

$$\arcsin(x) + \arccos(x) = \varphi + \frac{\pi}{2} - \varphi = \frac{\pi}{2}.$$

□

## 6.8 Présentation analytique rapide des fonctions cosh et sinh.

*Démonstration.*

- Domaine de définition et symétries.

sinh et cosh sont définies sur  $\mathbb{R}$ .

De plus,

(i)  $\forall x \in \mathbb{R}, -x \in \mathbb{R}$ ,

$$(ii) \forall x \in \mathbb{R}, \begin{cases} \sinh(-x) &= \frac{e^{-x} - e^x}{2} = -\frac{e^x - e^{-x}}{2} = -\sinh(x) \\ \text{et} \\ \cosh(-x) &= \frac{e^{-x} + e^{-(-x)}}{2} = \frac{e^x + e^{-x}}{2} = \cosh(x). \end{cases}$$

Donc sinh et cosh sont respectivement impaire et paire.

Nous les étudierons sur  $\mathbb{R}_+$  et pour les obtenir les graphes ( $\mathcal{C}_{\sinh}$  et  $\mathcal{C}_{\cosh}$ ) de ces fonctions sur  $\mathbb{R}$  à partir de ceux ( $\mathcal{C}_{\sinh}^+$  et  $\mathcal{C}_{\cosh}^+$ ) obtenus sur  $\mathbb{R}_+$ , nous le compléterons en traçant les images de ces graphes par la symétrie centrale  $s$  de centre  $O$  et par la réflexion  $r$  d'axe  $(O, \vec{j})$  :

$$\mathcal{C}_{\sinh} = \mathcal{C}_{\sinh}^+ \cup s(\mathcal{C}_{\sinh}^+) \quad \text{et} \quad \mathcal{C}_{\cosh} = \mathcal{C}_{\cosh}^+ \cup r(\mathcal{C}_{\cosh}^+)$$

- Variations : triviales.
- Branches infinies en  $+\infty$  et position relative de  $\mathcal{C}_{\sinh}$  et  $\mathcal{C}_{\cosh}$ .

$$\frac{\cosh(x)}{x} = \underbrace{\frac{e^x}{x}}_{\xrightarrow{x \rightarrow +\infty} +\infty} + \underbrace{\frac{e^{-x}}{x}}_{\xrightarrow{x \rightarrow +\infty} 0} \xrightarrow{x \rightarrow +\infty} +\infty$$

Donc le graphe de cosh admet une branche parabolique de direction asymptotique  $(O, \vec{j})$ .

On a :

$$\forall x \in \mathbb{R}, \quad \cosh(x) - \sinh(x) = e^{-x} \xrightarrow{x \rightarrow +\infty} 0^+$$

Donc les graphes des deux fonctions se rapprochent l'un de l'autre arbitrairement près lorsque  $x \rightarrow +\infty$ , et le graphe de cosh est au-dessus de celui de sinh.

- Tangente au graphe de sinh à l'origine et position relative.

Il s'agira d'étudier  $g : x \in \mathbb{R}_+ \mapsto \sinh(x) - x$ , de remarquer sa dérivabilité d'en étudier les variations puis de conclure, en précisant que cette étude révèle l'inflexion du graphe de sinh en 0.

□



## 7 Semaine 7

### 7.1 Calcul de $\int_0^{2\pi} e^{imt} dt$ en fonction de $m \in \mathbb{Z}$ . En Dédurre qu'une fonction polynomiale nulle sur un cercle centré en l'origine a tous ses coefficients nuls.

*Démonstration.* Soit  $m \in \mathbb{Z}$  fq. Calculons :

$$\frac{1}{2\pi} \int_0^{2\pi} e^{imt} dt$$

Si  $m \neq 0$  :

$$\begin{aligned} \frac{1}{2\pi} \int_0^{2\pi} e^{imt} dt &= \frac{1}{2\pi} \left[ \frac{e^{imt}}{im} \right]_0^{2\pi} \\ &= \frac{1}{2\pi} \left( \frac{1}{im} - \frac{1}{im} \right) = 0 \end{aligned}$$

Si  $m = 0$  :

$$\frac{1}{2\pi} \int_0^{2\pi} e^{imt} dt = \frac{1}{2\pi} \int_0^{2\pi} dt = \frac{2\pi}{2\pi} = 1$$

Donc

$$\frac{1}{2\pi} \int_0^{2\pi} e^{imt} dt = \begin{cases} 1 & \text{si } m = 0 \\ 0 & \text{si } m \neq 0 \end{cases}$$

Soit  $n \in \mathbb{N}$  fq

Soient  $(a_0, \dots, a_n) \in \mathbb{C}^{n+1}$  les coefficients de  $P(z) = \sum_{k=0}^n a_k z^k$ , et  $s \in \mathbb{Z}$ , et  $r \in \mathbb{R}_+^*$  fq. tels que  $P$  soit nulle lorsqu'elle est évaluée sur  $\mathcal{C}(0, r)$

$$\begin{aligned} \frac{1}{2\pi} \int_0^{2\pi} P(re^{it}) e^{-imt} dt &= \frac{1}{2\pi} \int_0^{2\pi} \left( \sum_{k=0}^n a_k (re^{it})^k \right) e^{-imt} dt \\ &= \sum_{k=0}^n a_k r^k \underbrace{\int_0^{2\pi} \frac{e^{it(k-s)}}{2\pi} dt}_{I_k} \end{aligned}$$

On remarque que :

— Si  $s \notin \llbracket 0, n \rrbracket$ ,  $\{k \in \llbracket 0, n \rrbracket \mid k = s\} = \emptyset$ , Donc

$$\sum_{k \in \llbracket 0, n \rrbracket} a_k s^k I_k = \sum_{\substack{k \in \llbracket 0, n \rrbracket \\ k=s}} a_k r^k = 0$$

— Si  $s \in \llbracket 0, n \rrbracket$ ,  $\{k \in \llbracket 0, n \rrbracket \mid k = s\} = s$ , Donc

$$\sum_{k \in \llbracket 0, n \rrbracket} a_k s^k I_k = \sum_{\substack{k \in \llbracket 0, n \rrbracket \\ k=s}} a_k s^k = a_s r^s$$

Or, puisque  $P$  s'annule sur le cercle de rayon  $r$  et de centre 0,  $\mathcal{C}(0, r)$ , ces sommes sont aussi nulles. On en déduit, en particulierisant pour un  $s \in \llbracket 0, n \rrbracket$  fixé quelconque que :

$$\sum_{k \in \llbracket 0, n \rrbracket} a_k s^k I_k = a_s r^s = 0 \implies a_s = 0$$

Donc

$$(\exists r \in \mathbb{R}_+^* : \forall \theta \in \mathbb{R}, P(re^{i\theta}) = 0) \implies \forall s \in \llbracket 0, n \rrbracket$$

Pour la preuve réciproque, soit  $n \in \mathbb{N}$  fq. Soient  $(a_0, \dots, a_n) \in \{0\}^{n+1}$  les coefficients nuls de la fonction polynomiale  $P \in \mathbb{C}[z]$  définie pour tout  $z \in \mathbb{C}$ .

En remarquant que  $\forall z \in \mathbb{C}, P(z) = 0$ , puisque n'importe quel cercle centré en 0 est un sous ensemble de  $\mathbb{C}$ ,  $\exists r \in \mathbb{R}_+^* : \forall z \in \mathcal{C}(0, r), P(z) = 0$ .  $\square$

## 7.2 Preuve de la Linéarité de la dérivation d'une fonction complexe

*Démonstration.* Définissons les fonctions  $f_r$  et  $f_i$  comme les parties réelles et imaginaires de  $f$ .

Soient  $(f, g) \in \mathcal{F}(I, \mathbb{C})^2$ ,  $(\alpha, \beta) \in \mathbb{C}^2$  fixés quelconques.

$$\begin{aligned} f_r &= \operatorname{Re}(f), f_i = \operatorname{Im}(f) & g_r &= \operatorname{Re}(g), g_i = \operatorname{Im}(g) \\ \alpha_r &= \operatorname{Re}(\alpha), \alpha_i = \operatorname{Im}(\alpha) & \beta_r &= \operatorname{Re}(\beta), \beta_i = \operatorname{Im}(\beta) \end{aligned}$$

$$\begin{aligned} \operatorname{Re}(\alpha f + \beta g) &= \operatorname{Re}((\alpha_r + i\alpha_i)(f_r + if_i) + (\beta_r + i\beta_i)(g_r + ig_i)) \\ &= \underbrace{\alpha_r f_r + \beta_r g_r - \alpha_i f_i - \beta_i g_i}_{\text{Combinaison linéaire de } (f_r, f_i, g_r, g_i) \in \mathcal{D}^1(I, \mathbb{R})^4} \\ &\quad \underbrace{\hspace{10em}}_{\operatorname{car}(f, g) \in \mathcal{D}^1(I, \mathbb{R})^2} \end{aligned}$$

Donc, selon le théorème de stabilité par combinaison linéaire des fonctions à valeurs réelles,  $\operatorname{Re}(\alpha f + \beta g) \in \mathcal{D}^1(I, \mathbb{R})$  et  $(\operatorname{Re}(\alpha f + \beta g))' = \alpha_r f_r' + \beta_r g_r' - \alpha_i f_i' - \beta_i g_i'$

On montre de même que  $\operatorname{Im}(\alpha f + \beta g) \in \mathcal{D}^1(I, \mathbb{R})$  et  $(\operatorname{Im}(\alpha f + \beta g))' = \alpha_r f_i' + \alpha_i f_r' + \beta_r g_i' + \beta_i g_r'$

Ainsi,

$$\begin{aligned} (\alpha f + \beta g)' &= (\alpha_r f_r' + \beta_r g_r' - \alpha_i f_i' - \beta_i g_i') + i(\alpha_r f_i' + \alpha_i f_r' + \beta_r g_i' + \beta_i g_r') \\ &= \alpha_r (f_r' + if_i') + \beta_r (g_r' + ig_i') + \alpha_i \underbrace{(-f_i' + if_r')}_{i(f_r' + if_i')} + \beta_i \underbrace{(-g_i' + ig_r')}_{i(g_r' + ig_i')} \\ &= \alpha f' + \beta g' \end{aligned}$$

□

## 7.3 Dérivée composée d'une fonction à valeurs complexes

*Démonstration.* Soient  $f \in \mathcal{D}^1(J, \mathbb{C})$  et  $h \in \mathcal{D}^1(I, J)$  ( $I$  et  $J$  sont deux intervalles réels) fixés quelconques. Notons  $f_r$  et  $f_i$  respectivement la partie réelle et imaginaire de  $f$ .

$$\left. \begin{aligned} h &\in \mathcal{D}^1(I, J) \\ f_r &\in \mathcal{D}^1(J, \mathbb{R}), \text{ car } f \in \mathcal{D}^1(J, \mathbb{C}) \end{aligned} \right\} \implies f_r \circ h \in \mathcal{D}^1(I, \mathbb{R})$$

On montre de même que  $f_i \circ h \in \mathcal{D}^1(I, \mathbb{R})$  donc  $f \circ h \in \mathcal{D}^1(I, \mathbb{C})$ .

De plus,

$$\begin{aligned} (f \circ h)' &= (f_r \circ h)' + i(f_i \circ h)' \\ &= (f_r' \circ h) \times h' + i((f_i' \circ h) \times h') \\ &= (f_r' \circ h + if_i' \circ h) \times h' \\ &= (f' \circ h) \times h' \end{aligned}$$

□

## 7.4 Caractérisation des fonctions dérivables de dérivée nulle sur un intervalle

*Démonstration.* Soit  $f \in \mathcal{D}^1(I, \mathbb{C})$  où  $I$  est un intervalle réel; Posons  $f_r = \operatorname{Re}(f)$  et  $f_i = \operatorname{Im}(f)$ .

$$\begin{aligned} \forall t \in I, f'(t) = 0 &\iff \forall t \in I, f_r'(t) + if_i'(t) = 0 \\ &\iff \begin{cases} \forall t \in I, f_r'(t) = 0 \\ \forall t \in I, f_i'(t) = 0 \end{cases} \\ &\iff \begin{cases} \exists \lambda_r \in \mathbb{R} : \forall t \in I, f_r(t) = \lambda_r \\ \exists \lambda_i \in \mathbb{R} : \forall t \in I, f_i(t) = \lambda_i \end{cases} \\ &\iff \exists \lambda \in \mathbb{C} : \forall t \in I, f(t) = \lambda \end{aligned}$$

□

## 8 Semaine 8

### 8.1 Preuve de l'expression des solutions réelles des EDL homogènes d'ordre 2 à coefficients constants réels dans le cas $\Delta < 0$ (en admettant la connaissance de l'expression des solutions à valeurs complexes des EDLH2 à coeff. constants).

*Démonstration.* Notons  $\mathcal{S}_{H,\mathbb{C}}$  et  $\mathcal{S}_{H,\mathbb{R}}$  les ensembles des solutions complexes et réelles de l'équation différentielle, puisque nous nous plaçons dans le cas  $\Delta < 0$  et  $\alpha \pm i\beta$  les deux racines complexes conjuguées.

$$\mathcal{S}_{H,\mathbb{C}} = \left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{C} \\ t \mapsto \lambda e^{(\alpha+i\beta)t} + \mu e^{(\alpha-i\beta)t} \end{array} \middle| (\lambda, \mu) \in \mathbb{C}^2 \right\}$$

Montrons que  $\forall f \in \mathcal{S}_{H,\mathbb{C}}, \text{Re}(f) \in \mathcal{S}_{H,\mathbb{R}}$   
Soit  $f \in \mathcal{S}_{H,\mathbb{C}}$  fq.

$$f \in \mathcal{D}^2(\mathbb{R}, \mathbb{C}) \implies \text{Re}(f) \in \mathcal{D}^2(\mathbb{R}, \mathbb{R})$$

Et, de plus, par morphisme additif de  $\text{Re}$

$$a_2 \text{Re}(f)'' + a_1 \text{Re}(f)' + a_0 \text{Re}(f) = \text{Re}(a_2 f'' + a_1 f' + a_0 f) = 0$$

D'où, avec  $f : t \mapsto e^{(\alpha+i\beta)t}$ ;  $\text{Re}(f(t)) = \text{Re}(e^{(\alpha+i\beta)t}) = e^{\alpha t} \cos(\beta t)$ . Qui appartient donc à  $\mathcal{S}_{H,\mathbb{R}}$   
En suivant le même raisonnement pour  $\text{Im}(f)$ , ( $t \mapsto e^{\alpha t} \sin(\beta t)$ )  $\in \mathcal{S}_{H,\mathbb{R}}$

Ainsi, par combinaison linéaire (qui se base sur le principe de superposition),

$$\left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ t \mapsto \lambda e^{\alpha t} \cos(\beta t) + \mu e^{\alpha t} \sin(\beta t) \end{array} \middle| (\lambda, \mu) \in \mathbb{R}^2 \right\} \subset \mathcal{S}_{H,\mathbb{R}}$$

Réciproquement, soit  $f \in \mathcal{S}_{H,\mathbb{R}}$  fq. Puisque  $\mathbb{R} \subset \mathbb{C}$ ,  $f \in \mathcal{S}_{H,\mathbb{C}}$ .

$$\exists (a, b) \in \mathbb{C}^2 : f \left| \begin{array}{l} \mathbb{R} \rightarrow \mathbb{C} \\ t \mapsto a e^{(\alpha+i\beta)t} + b e^{(\alpha-i\beta)t} \end{array} \right.$$

Or, puisque toutes les valeurs de  $f$  sont réelles, en notant  $(a_r, a_i, b_r, b_i)$  les parties réelles et imaginaires respectives de  $a$  et  $b$ .

$$\begin{aligned} \forall t \in \mathbb{R}, f(t) &= \text{Re}(f(t)) \\ &= \text{Re}(a e^{(\alpha+i\beta)t} + b e^{(\alpha-i\beta)t}) \\ &= \text{Re}((a_r + i a_i) e^{(\alpha+i\beta)t} + (b_r + i b_i) e^{(\alpha-i\beta)t}) \\ &= a_r \cos(\beta t) e^{\alpha} - a_i \sin(\beta t) e^{\alpha} + b_r \cos(\beta t) e^{\alpha} + b_i \sin(\beta t) e^{\alpha} \\ &= (a_r + b_r) \cos(\beta t) e^{\alpha} + (b_i - a_i) \sin(\beta t) e^{\alpha} \end{aligned}$$

Ainsi,

$$f \in \left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ t \mapsto \lambda e^{\alpha t} \cos(\beta t) + \mu e^{\alpha t} \sin(\beta t) \end{array} \middle| (\lambda, \mu) \in \mathbb{R}^2 \right\}$$

Ce qui conclut la preuve par double inclusion. □

### 8.2 Existence et unicité d'une solution au problème de Cauchy pour les EDL d'ordre 2 à coefficients constants et second membre continu sur $I$ (cas complexe puis cas réel).

Considérons le problème de Cauchy suivant :

$$\left\{ \begin{array}{l} a_2 y'' + a_1 y' + a_0 y = b \text{ sur } J \\ y(t_0) = \alpha_0 \\ y'(t_0) = \alpha_1 \end{array} \right. \quad \text{où } (\alpha_0, \alpha_1) \in \mathbb{K}^2, t_0 \in J, (a_0, a_1, a_2) \in \mathbb{K}^2 \times \mathbb{K}^*, b \in \mathcal{F}(J, \mathbb{K})$$

Si  $b$  est continu sur  $J$ , alors ce problème de Cauchy admet une unique solution définie sur  $J$ .

*Démonstration. Cas 1.*  $\mathbb{K} = \mathbb{C}$

Nous savons que sous l'hypothèse de continuité de  $b$  sur  $J$ , les solutions de (EDL2) définies sur  $J$  constituent le plan affine  $S$  :

$$S = \{\lambda f_1 + \mu f_2 + s \mid (\lambda, \mu) \in \mathbb{C}^2\}$$

où  $s$  est une solution particulière de (EDL2),  $(f_1, f_2)$  sont deux solutions de (EDLH2) qui engendrent  $S_h$ . On a :

$$\begin{aligned} f : J \rightarrow \mathbb{C} \text{ est sol. du pb de Cauchy} &\iff \begin{cases} f \text{ sol de (EDL2) sur } J \\ f(t_0) = \alpha_0 \\ f'(t_0) = \alpha_1 \end{cases} \\ &\iff \begin{cases} f \in S \\ f(t_0) = \alpha_0 \\ f'(t_0) = \alpha_1 \end{cases} \\ &\iff \exists (\lambda, \mu) \in \mathbb{C}^2 : \begin{cases} f = \lambda f_1 + \mu f_2 + s \\ \lambda f_1(t_0) + \mu f_2(t_0) + s(t_0) = \alpha_0 \\ \lambda f_1'(t_0) + \mu f_2'(t_0) + s'(t_0) = \alpha_1 \end{cases} \\ &\iff \exists (\lambda, \mu) \in \mathbb{C}^2 : \begin{cases} f = \lambda f_1 + \mu f_2 + s \\ \lambda f_1(t_0) + \mu f_2(t_0) = \alpha_0 - s(t_0) \\ \lambda f_1'(t_0) + \mu f_2'(t_0) = \alpha_1 - s'(t_0) \end{cases} \end{aligned}$$

On en déduit donc que  $(\lambda, \mu)$  doit être solution d'un système linéaire (2,2). On a une unique solution si et seulement si les déterminant de ce système est nul.

Explicitons alors le déterminant de ce système, que l'on notera  $D$ .

$$D = \begin{vmatrix} f_1(t_0) & f_2(t_0) \\ f_1'(t_0) & f_2'(t_0) \end{vmatrix} = f_1(t_0) \cdot f_2'(t_0) - f_2(t_0) \cdot f_1'(t_0)$$

Notons  $\Delta$  le discriminant de l'équation caractéristique de (EDL2) ( $a_2 r^2 + a_1 r^1 + a_0 = 0$ ). On distingue alors deux cas selon la nullité ou non de  $\Delta$ . Traitons d'abord le cas  $\Delta \neq 0$ . On peut choisir :

$$\begin{aligned} f_1(t_0) &= e^{r_1 t_0} \text{ et } f_2(t_0) = e^{r_2 t_0} \\ f_1'(t_0) &= r_1 e^{r_1 t_0} \text{ et } f_2'(t_0) = r_2 e^{r_2 t_0} \end{aligned}$$

Donc (en sachant que  $\Delta \neq 0 \Rightarrow r_1 \neq r_2$ ) :

$$D = e^{r_1 t_0} \cdot r_2 e^{r_2 t_0} - r_1 e^{r_1 t_0} \cdot e^{r_2 t_0} = (r_2 - r_1) \cdot e^{r_1 t_0 + r_2 t_0} \neq 0$$

Dans le deuxième cas, on a  $\Delta = 0$ ; on peut alors prendre :

$$f_1(t_0) = e^{r_0 t_0} \text{ et } f_2(t_0) = t_0 e^{r_0 t_0}$$

Ainsi :

$$D = e^{r_0 t_0} (r_0 t_0 e^{r_0 t_0} + e^{r_0 t_0}) - r_0 e^{r_0 t_0} \times t_0 e^{r_0 t_0} = e^{2r_0 t_0} \neq 0$$

On remarque alors que, dans les deux cas,  $D \neq 0$ , donc le système (2,2) étudié admet une unique solution, donc il existe un unique couple  $(\lambda, \mu)$  le vérifiant d'où l'unicité et existence d'une solution au problème de Cauchy.

**Cas 2.**  $\mathbb{K} = \mathbb{R}$

$(a_0, a_1, a_2) \in \mathbb{R}^2 \times \mathbb{R}^*$ ,  $(\alpha_0, \alpha_1) \in \mathbb{R}^2$ ,  $b \in C^0(J, \mathbb{R})$

**Existence :** Puisque  $\mathbb{R} \subset \mathbb{C}$ , le problème de Cauchy admet, dans  $\mathbb{R}$ , une solution à valeurs complexes  $g$ . Posons  $f = \text{Re}(g)$  et montrons que  $f$  est une solution réelle du problème de Cauchy.

$$\star \quad g \in \mathcal{D}^2(J, \mathbb{C}) \text{ donc } f \in \mathcal{D}^2(J, \mathbb{R})$$

★  $g$  vérifie  $a_2 g'' + a_1 g' + a_0 g = b$  sur  $J$  donc en prenant  $\text{Re}(\cdot)$  :

$$\text{Re}(a_2 g'' + a_1 g' + a_0 g = b) = \text{Re}(b) \iff a_2 \text{Re}(g'') + a_1 \text{Re}(g') + a_0 \text{Re}(g) = b$$

$$\iff a_2 f'' + a_1 f' + a_0 f = b \text{ sur } J$$

★  $f(t_0) = \text{Re}(g(t_0)) = \text{Re}(\alpha_0) = \alpha_0$

★  $f'(t_0) = \text{Re}(g(t_0))' = \text{Re}(g'(t_0)) = \text{Re}(\alpha_1) = \alpha_1$

Donc  $f$  est une solution réelle définie sur  $J$  au problème de Cauchy.

**Unicité :** Soient  $f_1$  et  $f_2$  deux fonctions à valeurs réelles solutions du problème de Cauchy ci-dessus fixées quelconques : puisque  $\mathbb{R} \subset \mathbb{C}$ ,  $f_1$  et  $f_2$  sont des fonctions à valeurs dans  $\mathbb{C}$  solutions du même problème de Cauchy ; or il y a unicité de la solution au problème de Cauchy dans les fonctions à valeurs complexes, donc  $f_1 = f_2$  dans  $\mathcal{F}(J, \mathbb{C})$ , donc  $f_1 = f_2$  dans  $\mathcal{F}(J, \mathbb{R})$ .  $\square$

### 8.3 Les solutions d'une EDL<sub>2</sub> constituent un espace vectoriel.

Soient  $(a, b) \in \mathbb{C}^2$ ,  $f$  et  $g$  les solutions, définies sur  $\mathbb{R}$  à valeurs dans  $\mathbb{C}$ , des problèmes de Cauchy suivants :

$$\begin{cases} y'' + ay' + by = 0 \\ y(3) = 1 \\ y'(3) = 0 \end{cases} \quad \text{et} \quad \begin{cases} y'' + ay' + by = 0 \\ y(3) = 0 \\ y'(3) = 1 \end{cases}$$

Comment s'exprime la solution définie sur  $\mathbb{R}$  de  $\begin{cases} y'' + ay' + by = 0 \\ y(3) = \alpha \\ y'(3) = \beta \end{cases}$  pour  $(\alpha, \beta) \in \mathbb{R}^2$  fixés ?

Peut-on affirmer que le plan vectoriel des solutions définies sur  $\mathbb{R}$  à valeurs dans  $\mathbb{C}$  de  $y'' + ay' + by = 0$  est  $\{\lambda \cdot f + \mu \cdot g \mid (\lambda, \mu) \in \mathbb{C}^2\}$

*Démonstration.* La solution s'exprime simplement comme combinaison linéaire de  $f$  et  $g$ , plus précisément, la combinaison linéaire en  $\alpha$  et  $\beta$ . En effet, soient de tels scalaires, et soient  $f$  et  $g$  de telles solutions, on a :

$$(\alpha \cdot f + \beta \cdot g)'' + a(\alpha \cdot f + \beta \cdot g)' + b(\alpha \cdot f + \beta \cdot g) = 0, \text{ par définition des espaces vectoriels.}$$

Et de même,  $(\alpha \cdot f + \beta \cdot g)'(3) = \alpha \cdot f'(3) + \beta \cdot g'(3) = \alpha$ , et  $(\alpha \cdot f + \beta \cdot g)''(3) = \alpha \cdot f''(3) + \beta \cdot g''(3) = \beta$ . Ce qui suffit par unicité des solutions ( de la donc ) d'un problème de Cauchy dans le cadre du théorème du cours.

Pour ce qui est du plan vectoriel des solutions, noté  $\Omega$ , notons aussi  $\Phi$  l'ensemble proposé. L'inclusion  $\Phi \subset \Omega$  est triviale par propriété de linéarité des espaces vectoriels. Finalement, pour  $\Omega \subset \Phi$ , soit  $\omega \in \Omega$ , forcément,  $\omega$  vérifie l'EDL<sub>2</sub>, mais aussi des conditions de Cauchy bien que celles-ci soient non-spécifiées, ainsi posons  $\omega'(3) = \delta$  et  $\omega''(3) = \theta$ , donc en particulier,  $\omega = \delta \cdot f + \theta \cdot g$ , d'où l'égalité par double inclusion.  $\square$

### 8.4 Formules de Cramer pour les systèmes $2 \times 2$

Résolution générale des systèmes linéaires à 2 équations et 2 inconnues en fonction du déterminant du système (**tous les cas ne sont pas nécessairement à envisager**)

Considérons le système linéaire à deux équations et à deux inconnues  $(x, y)$  :

$$(S) \begin{cases} ax + by = b_1 & (E_1) \\ cx + dy = b_2 & (E_2) \end{cases} \quad (2)$$

dont  $(a, b, c, d) \in \mathbb{K}^4$  sont les coefficients et  $(b_1, b_2) \in \mathbb{K}^2$  sont les seconds membres.

- (S) admet une unique solution si et seulement si  $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \neq 0$ . De plus, dans ce cas, la solution est

$$\left( \frac{\begin{vmatrix} b_1 & b \\ b_2 & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}, \frac{\begin{vmatrix} a & b_1 \\ c & b_2 \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}} \right) \quad (3)$$

- Si  $ad - bc = 0$ , alors l'ensemble des solutions est soit vide, soit une droite affine de  $\mathbb{K}^2$ , soit  $\mathbb{K}^2$ .

*Démonstration.* Procédons par disjonction de cas.

- Supposons que  $ad - bc \neq 0$ .
- Supposons que  $a \neq 0$ .

$$\begin{aligned}
 (S) &\iff \begin{cases} ax + by = b_1 \\ (d - \frac{bc}{a})y = b_2 - \frac{c}{a}b_1 \quad (L_1 \leftarrow L_1 - \frac{c}{a}L_2) \end{cases} \\
 &\iff \begin{cases} ax + by = b_1 \\ (ad - bc)y = ab_2 - cb_1 \quad (L_1 \leftarrow aL_1) \end{cases} \\
 &\iff \begin{cases} ax = \frac{1}{a} \left( b_1 - b \frac{ab_2 - cb_1}{ad - bc} \right) = \frac{1}{a} \frac{adb_1 - bcb_1 + abb_2 - bcb_2}{ad - bc} \\ y = \frac{ab_2 - cb_1}{ad - bc} \end{cases} \\
 &\iff \begin{cases} ax = \frac{db_1 - bb_2}{ad - bc} = \frac{\begin{vmatrix} b_1 & b \\ b_2 & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}} \\ y = \frac{ab_2 - cb_1}{ad - bc} = \frac{\begin{vmatrix} a & b_1 \\ c & b_2 \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}} \end{cases}
 \end{aligned}$$

Donc le système admet une unique solution qui est celle annoncée.

- Supposons que  $a = 0$ . L'hypothèse  $ad - bc \neq 0$  implique  $bc \neq 0$  donc  $b \neq 0$  et  $c \neq 0$ .

$$\begin{aligned}
 (S) &\iff \begin{cases} by = b_1 \\ cx + dy = b_2 \end{cases} \\
 &\iff \begin{cases} x = \frac{1}{c} \left( b_2 - d \frac{b_1}{b} \right) \\ y = \frac{b_1}{b} \end{cases} \\
 &\iff \begin{cases} ax = \frac{db_1 - bb_2}{-bc} = \frac{\begin{vmatrix} b_1 & b \\ b_2 & d \end{vmatrix}}{\begin{vmatrix} 0 & b \\ c & d \end{vmatrix}} \\ y = \frac{-cb_1}{-bc} = \frac{\begin{vmatrix} 0 & b_1 \\ c & b_2 \end{vmatrix}}{\begin{vmatrix} 0 & b \\ c & d \end{vmatrix}} \end{cases}
 \end{aligned}$$

Donc le système admet une unique solution qui est celle annoncée.

$$ad - bc = 0.$$

- Supposons  $a \neq 0$ . En reprenant la méthode pivot de Gauss,

$$\begin{aligned}
 (S) &\iff \begin{cases} ax + by = b_1 \\ (d - \frac{bc}{a})y = b_2 - \frac{c}{a}b_1 \quad (L_1 \leftarrow L_1 - \frac{c}{a}L_2) \end{cases} \\
 &\iff \begin{cases} ax + \underbrace{(ad - bc)}_0 y = ab_2 - cb_1 \quad (L_1 \leftarrow aL_1) \end{cases}
 \end{aligned}$$

Donc le système est de rang 1 avec une condition de compatibilité.

Si  $ab_2 - cb_1 \neq 0$ , (S) n'admet aucune solution.

Sinon  $ab_2 - cb_1 = 0$

$$(S) \iff ax + by = b_1 \iff \begin{pmatrix} x \\ y \end{pmatrix} \in \left\{ \begin{pmatrix} \frac{b_1}{a} - b \frac{t}{a} \\ t \end{pmatrix} \mid t \in \mathbb{K} \right\} \quad (4)$$

Donc (S) admet une droite affine de solutions.

- Supposons  $a = 0$ . Puisque  $ad - bc = 0$ , alors  $bc = 0$  donc  $b$  ou  $c$  est nul.
- Si  $c = 0$ ,

$$(S) \iff \begin{cases} by = b_1 \\ dy = b_2 \end{cases}$$

- Si  $b = 0$ ,

$$(S) \iff \begin{cases} by &= b_1 \\ 0 &= b_2 \end{cases}$$

- Si  $b_2 = 0$ , (S) n'admet aucune solution.

- Si  $b_2 \neq 0$ ,  $(S) \iff dy = b_2$

- Si  $d = 0$ ,  $(S) \iff 0 = b_2$ . (S) n'admet aucune solution ( $b_2 \neq 0$ ) ou admet  $\mathbb{K}^2$  comme ensemble des solutions ( $b_2 = 0$ ).

- Si  $d \neq 0$ ,  $(S) \iff y = \frac{b_2}{d} \iff \begin{pmatrix} x \\ y \end{pmatrix} \in \left\{ \begin{pmatrix} t \\ \frac{b_2}{d} \end{pmatrix} \mid t \in \mathbb{K} \right\}$ . Donc (S) admet une droite affine de solutions.

- Si  $b \neq 0$

$$(S) \iff \begin{cases} y &= \frac{b_1}{b} \\ 0 &= b_2 - \frac{db_1}{b} \end{cases}$$

- Si  $b_2 - \frac{db_1}{b} \neq 0$ , (S) n'admet aucune solution.

- Si  $b_2 - \frac{db_1}{b} = 0$ ,  $(S) \iff y = \frac{b_1}{b} \iff \begin{pmatrix} x \\ y \end{pmatrix} \in \left\{ \begin{pmatrix} t \\ \frac{b_1}{b} \end{pmatrix} \mid t \in \mathbb{K} \right\}$  donc (S) admet une droite affine de solutions.

- Si  $c \neq 0$  alors  $b = 0$

$$(S) \iff \begin{cases} 0 &= b_1 \\ cx + dy &= b_2 \end{cases}$$

- Si  $b_1 \neq 0$ , (S) n'admet aucune solution.

- Si  $b_1 = 0$ ,  $(S) \iff x = \frac{b_2}{c} - \frac{d}{c}y \iff \begin{pmatrix} x \\ y \end{pmatrix} \in \left\{ \begin{pmatrix} \frac{b_2}{c} - \frac{d}{c}t \\ t \end{pmatrix} \mid t \in \mathbb{K} \right\}$  donc (S) admet une droite affine de solutions.

□

## 9 Semaine 9

### 9.1 Deux classes d'équivalence sont disjointes ou confondues. Les classes d'équivalence constituent une partition de l'ensemble sur lequel on considère la relation d'équivalence.

Soit  $\mathcal{R}$  une relation d'équivalence sur  $E$ .

Soit  $x \in E$ .

La classe de  $x$ , notée  $\bar{x}$ , est l'ensemble des éléments de  $E$  en relation avec  $x$ .

$$\bar{x} = \{y \in E \mid x\mathcal{R}y\} \quad (5)$$

*Démonstration. Montrons que deux classes d'équivalence sont disjointes ou confondues.*

Soit  $(x, y) \in E^2$  fq.

- Si  $\bar{x} \cap \bar{y} = \emptyset$ , rien à démontrer.
- Sinon  $\bar{x} \cap \bar{y} \neq \emptyset$  donc  $\exists z \in \bar{x} \cap \bar{y}$ . Fixons un tel  $z$ .  
Soit  $x' \in \bar{x}$  fq.

$$\left. \begin{array}{l} x' \in \bar{x} \implies x\mathcal{R}x' \xRightarrow{\text{symétrie}} x'\mathcal{R}x \\ z \in \bar{x} \implies x\mathcal{R}z \\ z \in \bar{y} \implies y\mathcal{R}z \xRightarrow{\text{symétrie}} z\mathcal{R}y \end{array} \right\} \xRightarrow{\text{transitivité}} x'\mathcal{R}z \left\} \xRightarrow{\text{transitivité}} x'\mathcal{R}y \xRightarrow{\text{symétrie}} y\mathcal{R}x'$$

Donc  $x' \in \bar{y}$  donc  $\bar{x} \subset \bar{y}$ .

En échangeant les rôles de  $x$  et  $y$ , on montre la deuxième inclusion  $\bar{y} \subset \bar{x}$ .

*Montrons que les classes d'équivalence de  $E$  constituent une partition de  $E$ .*

Soit  $\mathcal{S}$  un système de représentant des classes fixé quelconque.

- Soit  $s \in \mathcal{S}$  fq.  $\bar{s} \neq \emptyset$  car  $s\mathcal{R}s$  par réflexivité.
- Soit  $(s, s') \in \mathcal{S}^2$  fq. D'après la démonstration ci-dessus,  $\bar{s} \cap \bar{s}' = \emptyset$  ou  $\bar{s} = \bar{s}'$ . Si  $\bar{s} = \bar{s}'$  alors  $s$  et  $s'$  représente la même classe ce qui est impossible car un système de représentants des classes contient un unique représentant de chaque classe. Par conséquent,  $\bar{s}$  et  $\bar{s}'$  sont disjoints.
- $\bigcup_{s \in \mathcal{S}} \bar{s} \subset E$  car  $\forall s \in \mathcal{S}, \bar{s} \subset E$  par définition d'une classe d'équivalence.  
Réciproquement, soit  $x \in E$  fq.  
Par réflexivité de  $\mathcal{R}$ ,  $x \in \bar{x}$ .  
Par définition d'un système de classe  $\exists! s_x \in \mathcal{S} : s_x \in \bar{x}$  donc  $\bar{s}_x = \bar{x}$ . Donc  $x \in \bar{s}_x \subset \bigcup_{s \in \mathcal{S}} \bar{s}$ .  
Donc  $E \subset \bigcup_{s \in \mathcal{S}} \bar{s}$ .  
Par double inclusion,  $E = \bigcup_{s \in \mathcal{S}} \bar{s}$ .

Ainsi,

$$E = \coprod_{s \in \mathcal{S}} \bar{s} \quad (6)$$

□

### 9.2 Si $A$ admet un plus grand élément c'est aussi sa borne supérieure. Si $A$ admet une borne supérieure dans $A$ c'est son plus grand élément.

Soit  $(E, \leq)$  un ensemble ordonné, et  $A$  une partie non-vidée de  $E$ .

Si  $A$  admet un plus grand élément alors  $A$  admet une borne supérieure et  $\sup A = \max A$ .

Si  $A$  admet une borne supérieure appartenant à elle-même alors  $A$  admet un plus grand élément et  $\max A = \sup A$ .



*Démonstration.* Soient un tel ensemble  $E$  et une telle partie  $A$  et notons  $M$  son plus grand élément. Posons l'ensemble des majorants de  $A$ ,  $M(A) = \{m \in E \mid \forall a \in A, a \leq m\}$ . Par définition :

$$\forall m \in M(A), M \leq m,$$

car  $M \in A$ , mais comme  $M \in M(A)$ , on a directement que  $M = \min M(A) = \sup A$ .

Pseudo-réciproquement, soit  $A$  une partie de  $E$  admettant une borne supérieure dans elle même, notons cette borne  $S$ .

Comme  $S \in M(A)$ , par définition,  $S$  est plus grand que tous les éléments de  $A$  mais appartient à  $A$ , donc de tous les éléments de  $A$ ,  $S$  est le plus grand.  $\square$

### 9.3 Théorème de la division Euclidienne dans $\mathbb{Z}$

$$\forall (a, b) \in \mathbb{Z}^2, \exists! (q, r) \in \mathbb{Z} \times \mathbb{N} : \begin{cases} a = bq + r \\ r \in \llbracket 0; |b| - 1 \rrbracket \end{cases} \quad (7)$$

*Démonstration. Unicité* Soient deux tels entiers  $(a, b) \in \mathbb{Z}^2$  et deux couples  $((q, r), (q', r')) \in (\mathbb{Z} \times \mathbb{N})^2$  tels que

$$\begin{cases} a = bq + r \\ 0 \leq r \leq |b| - 1 \end{cases} \quad \begin{cases} a = bq' + r' \\ 0 \leq r' \leq |b| - 1 \end{cases}$$

Directement,

$$b(q - q') = r' - r,$$

mais comme  $-(|b| - 1) \leq r' - r \leq |b| - 1$ , il vient en divisant par  $|b|$  l'inégalité précédente :

$$-1 < q - q' < 1,$$

puisque  $q$  et  $q'$  sont dans  $\mathbb{Z}$  leur différence est obligatoirement 0, ainsi  $q = q'$  ce qui implique  $r = r'$  et donc on a unicité de ladite écriture de  $a$ .

*Existence* Posons pour  $b \geq 1$ ,  $\Omega = \{k \in \mathbb{Z} \mid kb \leq a\}$

- $\Omega \subset \mathbb{Z}$
- non-vidé car  $-|a| \in \Omega$  ( $\mathbb{Z}$  archimédien suffit ...)
- $\Omega$  est majoré par  $|a|$  car supposons, par l'absurde, que  $\exists k \in \Omega : k > |a|$ , alors  $kb > |a|b > a$  ce qui contradiction avec la définition d' $\Omega$ .

Donc  $\Omega$  admet un plus grand élément, notons-le  $q$ .

Posons  $r = a - bq$ . Par construction,  $a = bq + r$  et comme  $q = \max \Omega$  et  $\Omega \subset \mathbb{Z}$ ,  $q \in \mathbb{Z}$  donc  $r \in \mathbb{Z}$ . Par suite,  $q \in \Omega$  donc  $bq \leq a$  d'où  $0 \leq r$ . Et  $q = \max \Omega$  donc  $b(q + 1) > a$  d'où  $b > r$ , c'est-à-dire,  $r \in \llbracket 0, |b| - 1 \rrbracket$ .

Si  $b < 1$ , il suffit de prendre  $q \leftarrow -q$  dans la preuve précédente. C'est donc l'existence de ladite écriture de  $a$ .  $\square$

### 9.4 Une suite décroissante et minorée de nombres entiers relatifs est stationnaire

*Démonstration.* Soit  $u \in \mathbb{Z}^{\mathbb{N}}$  une suite décroissante et minorée fixée quelconque.

Considérons  $A = \{u_n \mid n \in \mathbb{N}\}$  c'est-à-dire l'ensemble des valeurs prises par la suite  $u$ .

$A$  est :

- une partie de  $\mathbb{Z}$  car  $u$  est à valeur dans  $\mathbb{Z}$
- non vide car  $u_0 \in A$
- minoré car  $u$  est minorée

Donc  $A$  admet un plus petit élément. Donc  $\exists n_0 \in \mathbb{N} : u_{n_0} = \min A$ . Fixons un tel  $n_0$ .

Soit  $n \in \mathbb{N}$  tq  $n \geq n_0$ .

$$\left. \begin{array}{l} u_n \in A \implies u_n \geq \min A = u_{n_0} \\ u \text{ est décroissante et } n \geq n_0 \text{ donc } u_n \leq u_{n_0} \end{array} \right\} \implies u_n = u_{n_0}$$

Ainsi,  $u$  est stationnaire.  $\square$

## 10 Semaine 10

### 10.1 Caractérisation de la densité d'une partie $A$ de $\mathbb{R}$ dans une partie $B$ de $\mathbb{R}$ la contenant avec des $\varepsilon$ .

Soient  $(A, B) \in \mathcal{P}(\mathbb{R})^2$  fq.

*Définition de la densité*

$$A \text{ est dense dans } B \text{ si } \begin{cases} A \subset B \\ \text{et} \\ \forall (u, v) \in \mathbb{R}^2, B \cap ]u, v[ \neq \emptyset \implies A \cap ]u, v[ \neq \emptyset \end{cases} \quad (8)$$

*Caractérisation de la densité par les  $\varepsilon$*

$$A \text{ est dense dans } B \iff \begin{cases} A \subset B \\ \text{et} \\ \forall b \in B, \forall \varepsilon \in \mathbb{R}_+^*, \exists a \in A : |b - a| < \varepsilon \end{cases} \quad (9)$$

*Démonstration. Montrons la caractérisation de la densité*

*Sens Direct* Supposons  $A$  dense dans  $B$

— Par déf  $A \subset B$

— Soit  $b \in B$  et  $\varepsilon \in \mathbb{R}_+^*$  fq

Appliquons le (ii) de la déf de Densité pour  $u \leftarrow b - \varepsilon$  et  $v \leftarrow b + \varepsilon$

$$B \cap ]b - \varepsilon, b + \varepsilon[ \neq \emptyset \implies A \cap ]b - \varepsilon, b + \varepsilon[ \neq \emptyset$$

Or,  $B \cap ]b - \varepsilon, b + \varepsilon[ \neq \emptyset$  est vraie donc  $A \cap ]b - \varepsilon, b + \varepsilon[ \neq \emptyset$

Ce qui permet de choisir  $a \in A \cap ]b - \varepsilon, b + \varepsilon[$ . Un tel  $a$  vérifie  $a \in A$  et  $a \in ]b - \varepsilon, b + \varepsilon[ \iff |b - a| < \varepsilon$

$$\text{Sens réciproque Supposons } \begin{cases} A \subset B \\ \text{et} \\ \forall b \in B, \forall \varepsilon \in \mathbb{R}_+^*, \exists a \in A : |b - a| < \varepsilon \end{cases}$$

— On a donc  $A \subset B$

— Soient  $(u, v) \in \mathbb{R}^2$  fq tq  $B \cap ]u, v[ \neq \emptyset$

Soit  $b \in B \cap ]u, v[$  fq. Appliquons l'hypothèse pour  $b \leftarrow b$  et  $\varepsilon \leftarrow \min\{v - b, b - u\}$ , qui est autorisé  $v - b$  et  $b - u$  sont positifs

Donc  $\exists a \in A : |b - a| < \varepsilon$

Fixons un tel  $a$ , alors :

$$b - \varepsilon < a < b + \varepsilon$$

Donc

$$\begin{cases} a < b + \varepsilon = b + \underbrace{\min\{v - b, b - u\}}_{\leq v - b} \leq b + v - b = v \\ \text{et} \\ a > b - \varepsilon = b - \underbrace{\min\{v - b, b - u\}}_{\leq b - u} \geq b - (b - u) = u \end{cases}$$

Donc  $a \in ]u, v[$ .

Donc  $A \cap ]u, v[ \neq \emptyset$

□

### 10.2 Théorème de la division pseudo-euclidienne dans $\mathbb{R}$

$$\forall (a, b) \in \mathbb{R} \times \mathbb{R}^*, \exists !(q, r) \in \mathbb{Z} \times \mathbb{R} : \begin{cases} a = bq + r \\ r \in [0; |b|[ \end{cases} \quad (10)$$

*Démonstration. Unicité* Soient deux tels entiers  $(a, b) \in \mathbb{R}^2$  et deux couples  $((q, r), (q', r')) \in (\mathbb{Z} \times \mathbb{R})^2$  tels que

$$\begin{cases} a = bq + r \\ r \in [0; |b|[ \end{cases} \quad \begin{cases} a = bq' + r' \\ r' \in [0; |b|[ \end{cases}$$

Directement,

$$b(q - q') = r' - r,$$

mais comme  $-|b| < r' - r < |b|$ , il vient en divisant par  $|b|$  l'inégalité précédente :

$$-1 < q - q' < 1,$$

puisque  $q$  et  $q'$  sont dans  $\mathbb{Z}$  leur différence est obligatoirement 0, ainsi  $q = q'$  ce qui implique  $r = r'$  et donc on a unicité de ladite écriture de  $a$ .

*Existence* Posons pour  $b > 0$ ,  $\Omega = \{k \in \mathbb{Z} \mid kb \leq a\}$

—  $\Omega \subset \mathbb{Z}$

— non-vidé car  $-|a| \in \Omega$  ( $\mathbb{Z}$  archimédien suffit ...)

—  $\Omega$  est majoré par  $|a|$  car supposons, par l'absurde, que  $\exists k \in \Omega : k > |a|$ , alors  $kb > |a|b > a$  ce qui contradiction avec la définition d' $\Omega$ .

Donc  $\Omega$  admet un plus grand élément, notons-le  $q$ .

Posons  $r = a - bq$ . Par construction,  $a = bq + r$  et comme  $q = \max \Omega$  et  $r \in \mathbb{R}$ .

Par suite,  $q \in \Omega$  donc  $bq \leq a$  d'où  $0 \leq r$ . Et  $q = \max \Omega$  donc  $b(q + 1) > a$  d'où  $b > r$ , c'est-à-dire,  $r \in [0, |b|$ .

Si  $b < 0$ , il suffit de prendre  $q \leftarrow -q$  dans la preuve précédente. C'est donc l'existence de ladite écriture de  $a$ .  $\square$

### 10.3 $\mathbb{Q}$ est dense dans $\mathbb{R}$ et $\mathbb{R} \setminus \mathbb{Q}$ est aussi dense dans $\mathbb{R}$

*Démonstration.* Soit  $x \in \mathbb{R}$  fq. Posons  $\forall n \in \mathbb{N}, a_n = \frac{\lfloor 2^n x \rfloor}{2^n}$ .  
Soit  $n \in \mathbb{N}$  fq.

—  $a_n \in \mathbb{Q}$  car  $\lfloor 2^n x \rfloor \in \mathbb{Z}$  et  $2^n \in \mathbb{N}$ .

—

$$a_n = \frac{\lfloor 2^n x \rfloor}{2^n} \implies \frac{2^n x - 1}{2^n} \leq a_n \leq \frac{2^n x}{2^n} \implies x - \frac{1}{2^n} \leq a_n \leq x$$

Or  $1/2^n \xrightarrow{n \rightarrow +\infty} 0$  donc d'après le théorème d'existence de limite par encadrement,  
 $a_n \xrightarrow[n \rightarrow +\infty]{n \rightarrow +\infty} x$ .

Donc d'après la caractérisation séquentielle de la densité,  $\mathbb{Q}$  est dense dans  $\mathbb{R}$ .

Soit  $x \in \mathbb{R}$  fq.

Alors  $x + \sqrt{2} \in \mathbb{R}$ . D'après la démonstration précédente,  $\exists b \in \mathbb{Q}^{\mathbb{N}} : b_n \xrightarrow[n \rightarrow +\infty]{} x + \sqrt{2}$ .

Fixons une telle suite  $b$ . Considérons  $c = b - \sqrt{2}$ .

Soit  $n \in \mathbb{N}$  fq.

—  $c_n \in \mathbb{R} \setminus \mathbb{Q}$  car  $b_n \in \mathbb{Q}$  et  $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ .

—

$$\left. \begin{array}{l} b_n \xrightarrow[n \rightarrow +\infty]{} x + \sqrt{2} \\ c_n = b_n - \sqrt{2} \end{array} \right\} \implies c_n \xrightarrow[n \rightarrow +\infty]{} x$$

Donc d'après la caractérisation séquentielle de la densité,  $\mathbb{R} \setminus \mathbb{Q}$  est dense dans  $\mathbb{R}$ .  $\square$

### 10.4 Preuve de l'unicité de la limite d'une suite convergente

Soit  $u \in \mathbb{K}^{\mathbb{N}}, (\ell_1, \ell_2) \in \mathbb{K}^2$  Si  $u$  converge vers  $\ell_1$  et  $\ell_2$ , alors  $\ell_1 = \ell_2$

*Démonstration.* Par l'absurde, supposons que  $u$  converge vers  $\ell_1$  et  $\ell_2$ , et  $\ell_1 \neq \ell_2$ . On prendra  $\varepsilon_0 = \varepsilon_1 = \varepsilon_2$  assez petit pour que les tubes soient disjoints. Posons donc  $\varepsilon_0 = \frac{|\ell_1 - \ell_2|}{3}$

— Appliquons la définition de la convergence de  $u$  vers  $\ell_1$ , pour  $\varepsilon \leftarrow \varepsilon_0$ , ce qui est autorisé car  $\varepsilon_0 \in \mathbb{R}_+^*$

$$\exists N_1 \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N_1 \implies |u_n - \ell_1| \leq \varepsilon_0 \quad (11)$$

$$\exists N_2 \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N_2 \implies |u_n - \ell_2| \leq \varepsilon_0 \quad (12)$$

Fixons de tels  $N_1$  et  $N_2$ .

— Posons  $n_0 = N_1 + N_2$

—  $n_0 \geq N_1$ , donc (15) s'applique :  $|u_{n_0} - \ell_1| \leq \varepsilon_0$

—  $n_0 \geq N_2$ , donc (12) s'applique :  $|u_{n_0} - \ell_2| \leq \varepsilon_0$

—

$$\begin{aligned} |\ell_1 - \ell_2| &= |\ell_1 - u_{n_0} + u_{n_0} - \ell_2| \\ &\leq \underbrace{|\ell_1 - u_{n_0}|}_{\leq \varepsilon_0} + \underbrace{|u_{n_0} - \ell_2|}_{\leq \varepsilon_0} \\ &\leq 2 \frac{|\ell_1 - \ell_2|}{3} \\ \implies 1 &\leq \frac{2}{3} \end{aligned}$$

Contradiction

□

## 10.5 Une suite convergente est bornée

*Démonstration.* Soit  $u \in \mathbb{K}^{\mathbb{N}}$  convergente. Posons  $\ell = \lim u$  Appliquons la définition de la convergence pour  $\varepsilon \leftarrow 1$

$$\exists N_1 \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N_1 \implies |u_n - \ell| \leq 1$$

Fixons un tel  $N_1$  Posons alors  $M = \max \{|u_0|, |u_1|, |u_2| \dots |u_{N_1}|, |\ell| + 1\}$ , qui est bien défini, car toute partie finie, non vide d'un ensemble totalement ordonné (ici  $(\mathbb{R}, \leq)$ ) admet un pgE.

Soit  $n \in \mathbb{N}$  fq.

— Si  $n \in [0, N_1]$ ,  $|u_n| \in \{|u_0|, |u_1|, |u_2| \dots |u_{N_1}|, |\ell| + 1\}$  donc  $|u_n| \leq M$

— Sinon,

$$\begin{aligned} n > N_1 &\implies |u_n - \ell| \leq 1 \\ &\implies |u_n| - |\ell| \leq 1 \\ &\implies |u_n| \leq 1 + |\ell| \leq M \end{aligned}$$

Ainsi,  $\forall n \in \mathbb{N}, |u_n| \leq M$ .

□

## 11 Semaine 11

### 11.1 Caractérisation séquentielle de la densité.

Soient  $(A, B) \in (\mathcal{P}(\mathbb{R}) \setminus \{\emptyset\})^2$ . Montrons que :

$$A \text{ est dense dans } B \iff \begin{cases} A \subset B \\ \forall b \in B, \exists (a_n) \in A^{\mathbb{N}} : (a_n) \text{ converge vers } b \end{cases}$$

*Démonstration.* Sens indirect : supposons  $A \subset B$  et  $\forall b \in B, \exists (a_n) \in A^{\mathbb{N}} : (a_n) \text{ converge vers } b$  :

★  $A \subset B$  par hypothèse.

★ Montrons que  $\forall b \in B, \forall \varepsilon \in \mathbb{R}_+^*, \exists a \in A : |b - a| < \varepsilon$  (on utilise la caractérisation de la densité avec les  $\varepsilon$ )

Soient  $b \in B$  et  $\varepsilon \in \mathbb{R}_+^*$  fixés quelconques :

Par hypothèse appliquée pour  $b \leftarrow b : \exists (a_n) \in A^{\mathbb{N}} : a_n \xrightarrow{n \rightarrow +\infty} b$

Appliquons la définition de la convergence de  $(a_n)$  vers  $b$  pour  $\varepsilon \leftarrow \frac{\varepsilon}{2}$  :

$$\exists N \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N \Rightarrow |a_n - b| \leq \frac{\varepsilon}{2}$$

Fixons un tel  $N$  :

En particulier,  $a_N \in A$  et  $|a_N - b| \leq \frac{\varepsilon}{2} \leq \varepsilon$

Donc  $A$  est dense dans  $B$ .

Sens direct : supposons  $A$  dense dans  $B$  :

★ Par définition,  $A \subset B$

★ Soit  $b \in B$  fixé quelconque.

Soit  $n \in \mathbb{N}$  fixé quelconque :

Appliquons la caractérisation de la densité par les  $\varepsilon$  pour  $\varepsilon \leftarrow \frac{1}{2^n}$  (autorisé car  $\frac{1}{2^n} > 0$ ), et  $b \leftarrow b$  :

$$\exists a \in A : |a - b| \leq \frac{1}{2^n}$$

Notons  $a_n$  un tel élément. Nous venons de construire  $(a_n)_{n \in \mathbb{N}} \in A^{\mathbb{N}}$  vérifiant :

$$\forall n \in \mathbb{N}, |a_n - b| \leq \frac{1}{2^n}$$

$$\text{Or : } \lim_{n \rightarrow +\infty} \frac{1}{2^n} = 0$$

Ainsi, d'après le théorème sans nom,  $(a_n)_{n \in \mathbb{N}}$  converge vers  $b$ .

□

### 11.2 Théorème de la convergence monotone

Soit  $u \in \mathbb{R}^{\mathbb{N}}$  une suite monotone :

1. Si  $u$  est croissante

(i) Soit  $u$  est majorée, et dans ce cas,  $\lim u = \sup\{u_k | k \in \mathbb{N}\}$

(ii) Soit  $u$  n'est pas bornée, et dans ce cas,  $u$  diverge vers  $+\infty$ .

2. Si  $u$  est décroissante :

(i) Soit  $u$  est minorée, et dans ce cas,  $\lim u = \inf\{u_k | k \in \mathbb{N}\}$

(ii) Soit  $u$  n'est pas bornée, et dans ce cas,  $u$  diverge vers  $-\infty$ .

*Démonstration.* Soit  $u \in \mathbb{R}^{\mathbb{N}}$  monotone fq.

1. Supposons que  $u$  est croissante.

(i) Supposons que  $u$  est majorée.

Alors  $\exists M \in \mathbb{R} : \forall n \in \mathbb{N}, u_n \leq M$ . Fixons un tel  $M$ .

$\Omega = \{u_k | k \in \mathbb{N}\}$  est

— une partie de  $\mathbb{R}$

— non vide car  $u_0$  y appartient

— majorée par  $M$

donc elle admet une borne supérieure et notons-la  $\sigma$ .

Soit  $\epsilon \in \mathbb{R}_+^*$  fq.

$\sigma - \epsilon < \sigma$  donc  $\sigma - \epsilon$  ne majore pas  $\Omega$ . Donc  $\exists N \in \mathbb{N} : u_N > \sigma - \epsilon$ . Fixons un tel  $N$ .

Soit  $n \in \mathbb{N}$  fq tq  $n \geq N$ .

Alors  $u_n \underset{\text{par croissant de } u}{\geq} u_N \geq \sigma - \epsilon$  et  $u_n \underset{\text{par définition de } \sigma}{\leq} \sigma$ .

Ainsi,

$$\begin{aligned} \sigma - \epsilon \leq u_n \leq \sigma &\implies -\epsilon \leq u_n - \sigma \leq 0 \\ &\implies |u_n - \sigma| \leq \epsilon \end{aligned}$$

Donc  $u_n \xrightarrow{n \rightarrow +\infty} \sigma$ .

(ii) Supposons que  $u$  n'est pas bornée.

Soit  $A \in \mathbb{R}$  fq.

$u$  n'est pas bornée donc  $\exists N \in \mathbb{N} : u_N > A$ .

Or  $u$  est croissante donc  $\forall n \in \mathbb{N}, n \geq N \implies u_n \geq A$ .

Donc  $u_n \xrightarrow{n \rightarrow +\infty} +\infty$ .

2. Supposons que  $u$  est décroissante.

Il suffit dans la preuve ci-dessus de remplacer les inégalités inférieures par des inégalités supérieures et inversement et d'utiliser la notion de borne inférieure plutôt que de borne supérieure.

(i) Si  $u$  est minorée,  $u_n \xrightarrow{n \rightarrow +\infty} \inf\{u_k | k \in \mathbb{N}\}$ .

(ii) Si  $u$  n'est pas bornée,  $u_n \xrightarrow{n \rightarrow +\infty} -\infty$ .

□

### 11.3 Théorème de Césaro

Soit  $u \in \mathbb{R}^{\mathbb{N}}$  qui converge vers  $\ell \in \mathbb{R}$ .

Alors la moyenne arithmétique des  $n \in \mathbb{N}$  premiers termes (appelée moyenne de Césaro) converge vers  $\ell$ .

*Démonstration.* Soient  $u$  une telle suite,  $\epsilon \in \mathbb{R}_+^*$  et  $\ell \in \mathbb{R}$  ladite limite de  $u$ . Appliquons la définition de la convergence de  $u$  pour  $\epsilon \leftarrow \frac{\epsilon}{2}$  :

$$\exists N \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N \implies |u_n - \ell| \leq \frac{\epsilon}{2}.$$

Fixons un tel  $N$ . Posons  $\omega = \sum_{k=0}^{N-1} |u_k - \ell| \in \mathbb{R}$ . Soit  $n \in \mathbb{N}$  tel que  $n \geq N$ . Calculons :

$$\left| \frac{1}{n} \sum_{k=0}^{n-1} u_k - \ell \right| = \left| \frac{1}{n} \left( \sum_{k=0}^{n-1} u_k - n\ell \right) \right| = \left| \frac{1}{n} \sum_{k=0}^{n-1} (u_k - \ell) \right| \leq \underbrace{\frac{1}{n} \sum_{k=0}^{N-1} |u_k - \ell|}_{= \omega \in \mathbb{R}} + \underbrace{\frac{1}{n} \sum_{k=N}^n |u_k - \ell|}_{\leq \frac{\epsilon}{2}} \leq \frac{\omega}{n} + \underbrace{\frac{\epsilon}{2n}}_{\leq \frac{\epsilon}{2}}.$$

Ces majorations sont issues de l'inégalité triangulaire et de la convergence de  $u$ . De plus, comme la suite  $(v_n)_{n \in \mathbb{N}} = \left(\frac{\omega}{n}\right)_{n \in \mathbb{N}}$  converge vers 0, on écrit sa définition pour  $\epsilon \leftarrow \frac{\epsilon}{2}$  :

$$\exists N' \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N' \implies |v_n| \leq \frac{\epsilon}{2}.$$

On fixe un tel  $N'$  et on pose  $\Lambda = \max(N, N')$  qui a bien un sens car  $\{N, N'\}$  est une partie finie de  $\mathbb{N}$ . De la même manière qu'auparavant, pour  $n \in \mathbb{N}$  tel que  $n \geq \Lambda$ , on a :

$$\left| \frac{1}{n} \sum_{k=0}^{n-1} u_k - \ell \right| \leq \underbrace{\frac{\omega}{n}}_{\leq \frac{\epsilon}{2}} + \frac{\epsilon}{2} \leq \epsilon.$$

C'est le théorème souhaité.

□

## 11.4 Théorème de passage à la limite dans une inégalité.

Soient  $(u, v) \in \mathbb{R}^{\mathbb{N}}$  :

- (i) Si  $\left| \begin{array}{l} \exists N \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N \Rightarrow u_n \geq 0 \\ u \text{ converge} \end{array} \right|$   
Alors  $\lim u \geq 0$
- (ii) Si  $\left| \begin{array}{l} \exists N \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N \Rightarrow u_n \leq v_n \\ u \text{ et } v \text{ convergent} \end{array} \right|$   
Alors  $\lim u \leq \lim v$

*Démonstration.*

- (i) L'hypothèse  $\exists N \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N \Rightarrow u_n \geq 0$  permet d'affirmer que  $u$  et  $|u|$  coïncident à partir d'un certain rang.  
Par ailleurs, la convergence de  $u$  et la continuité de  $|\cdot|$  sur  $\mathbb{R}$  donc en  $\lim u$  donnent  $|u|$  converge vers  $|\lim u|$ .  
Le caractère asymptotique de la limite permet de conclure que  $u$  et  $|u|$  ont la même limite.  
Donc  $\lim u = |\lim u| \geq 0$
- (ii)  $\exists N \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N \Rightarrow u_n \leq v_n \Rightarrow v_n - u_n \geq 0$   
 $u$  et  $v$  convergent  $\Rightarrow v - u$  converge vers  $\lim v - \lim u$ .  
On applique (i) pour  $u \leftarrow v - u$ , autorisé car  $u$  et  $v$  convergent.  
On obtient  $\lim v - \lim u \geq 0$  d'où  $\lim u \leq \lim v$ .

□

## 11.5 Théorème des suites adjacentes

Soient  $u$  et  $v$  deux suites réelles adjacentes. Alors  $u$  et  $v$  convergent et ont la même limite.

*Démonstration.* Soient  $u$  et  $v$  de telles suites. Quitte à inverser les rôles desdites suites, prenons  $u$  croissante et  $v$  décroissante.

On a donc :

$$\forall n \in \mathbb{N}, (u_n \leq v_n \leq \underbrace{v_0}_{\in \mathbb{R}}) \wedge (\underbrace{u_0}_{\in \mathbb{R}} \leq u_n \leq v_n),$$

car la monotonie des suites induit ces inégalités. D'après le théorème de limite monotone,  $u$  étant croissante et majorée elle converge,  $v$  étant décroissante et minorée elle converge.

Il s'en suit que par définition des suites adjacentes :

$$0 = \lim_{n \rightarrow +\infty} (u_n - v_n) \underset{\substack{u, v \\ \text{convergent}}}{=} \lim_{n \rightarrow +\infty} u_n - \lim_{n \rightarrow +\infty} v_n.$$

Ainsi,  $\lim u = \lim v$ .

□

## 11.6 *Facultative* Théorème de Bolzano-Weierstrass

Toute suite bornée réelle admet une sous-suite convergente.

L'ensemble des valeurs d'adhérence d'une suite réelle bornée est non vide.

*Démonstration.* Soit  $u \in \mathbb{R}^{\mathbb{N}}$  fq bornée.

Alors  $\exists M \in \mathbb{R}_+ : \forall n \in \mathbb{N}, |u_n| \leq M$ .

Construisons une suite de segments dans  $[-M; M]$  de plus en plus petits par dichotomie.

Posons  $a_0 = -M$ ,  $b_0 = M$  et définissons les suites  $c$  et  $I$  pour tout  $n$  dans  $\mathbb{N}$  par  $c_n = \frac{a_n + b_n}{2}$  et  $I_n = [a_n; b_n]$ .

Soit  $n \in \mathbb{N}$  fq. Supposons  $a_n$  et  $b_n$  construits et  $\{k \in \mathbb{N} \mid u_k \in I_n\}$  infini. Construisons les termes d'indices  $n+1$ .

$$\text{Posons } \left| \begin{array}{l} I_n^- = \{k \in \mathbb{N} \mid u_k \in [a_n; c_n]\} \\ I_n^+ = \{k \in \mathbb{N} \mid u_k \in [c_n; b_n]\} \end{array} \right|$$

Nous avons  $I_n^- \cup I_n^+ = \{k \in \mathbb{N} \mid u_k \in I_n\}$  donc  $I_n^-$  ou  $I_n^+$  est infini.

- Si  $I_n^-$  est infini, posons  $\begin{cases} a_{n+1} = a_n \\ b_{n+1} = c_n \end{cases}$ .  
Ainsi  $\{k \in \mathbb{N} \mid u_k \in I_{n+1}\} = I_n^-$  est infini.
- Si  $I_n^+$  est infini, posons  $\begin{cases} a_{n+1} = c_n \\ b_{n+1} = b_n \end{cases}$ .  
Ainsi  $\{k \in \mathbb{N} \mid u_k \in I_{n+1}\} = I_n^+$  est infini.

Étudions la suite  $(I_n)_{n \in \mathbb{N}}$ .

- Nous avons toujours  $a_n \leq b_n$  donc  $\forall n \in \mathbb{N}, I_n \neq \emptyset$
- Par construction,  $\forall n \in \mathbb{N}, I_{n+1} \subset I_n$
- $|I_{n+1}| = |a_{n+1} - b_{n+1}| = \frac{1}{2}|a_n - b_n| = \frac{1}{2}|I_n|$  donc la suite des cardinaux est une suite géométrique de raison  $1/2$ . Donc  $|I_n| \xrightarrow{n \rightarrow +\infty} 0$ .

Donc, d'après le théorème des segments emboîtés,  $\exists ! \ell \in \mathbb{R} : \bigcap_{n \in \mathbb{N}} I_n = \{\ell\}$ . Fixons un tel  $\ell$ .

Construisons maintenant une extractrice  $\varphi$  de  $u$ .

Posons  $\varphi(0) = 0$ .

Soit  $n \in \mathbb{N}$  f.q. Supposons  $\varphi(n)$  construite.

$$\varphi(n+1) = \min\{k \in \mathbb{N} \mid u_k \in I_{n+1} \wedge k > \varphi(n)\}$$

$\varphi(n+1)$  est bien définie car  $\{k \in \mathbb{N} \mid u_k \in I_{n+1}\}$  est une partie de  $\mathbb{N}$  non bornée (car infinie).

Ainsi, nous avons construit  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  strictement croissante. Nous pouvons extraire une sous-suite de  $u$ . Or  $\forall n \in \mathbb{N}, u_{\varphi(n)} \in I_n$  donc

$$\forall n \in \mathbb{N}, \quad \underbrace{a_n}_{\xrightarrow{n \rightarrow +\infty} \ell} \leq u_{\varphi(n)} \leq \underbrace{b_n}_{\xrightarrow{n \rightarrow +\infty} \ell}$$

Donc, d'après le théorème d'existence de limite par encadrement,  $u_{\varphi(n)} \xrightarrow{n \rightarrow +\infty} \ell$ .

Ainsi  $\ell \in L_u$ . □

## 11.7 *Facultative* Caractérisation de la convergence par l'unicité d'une valeur d'adhérence pour une suite bornée.

Soit  $u$  une suite bornée.  $u$  converge si et seulement si il existe  $\ell \in \mathbb{K}$  tel que  $L(u)$  est le singleton  $\ell$

*Démonstration.* Traitons le cas réel, celui sur  $\mathbb{C}$  est à adapter sans peine.

Supposons que  $u$  converge et posons  $\lim u = \ell \in \mathbb{R}$ . Toutes les sous-suites de  $u$  convergent vers  $\ell$  donc  $L(u) = \{\ell\}$ .

Supposons maintenant qu'il existe un unique  $\ell \in \mathbb{R}$  tel que  $L(u) = \{\ell\}$ . Par l'absurde, supposons que  $u$  ne converge pas vers  $\ell$ , c'est-à-dire :

$$\exists \varepsilon \in \mathbb{R}_+^* : \forall N \in \mathbb{N}, \exists n \in \mathbb{N} : n \geq N \text{ et } |u_n - \ell| > \varepsilon.$$

Fixons un tel  $\varepsilon$ .

Posons  $\varphi(0) = \min\{k \in \mathbb{N} \mid |u_k - \ell| > \varepsilon\}$ , ce qui a du sens car c'est une partie non-vide de  $\mathbb{N}$ . Posons ensuite  $\varphi(1) = \min\{k \in \mathbb{N} \mid |u_k - \ell| > \varepsilon, \varphi(0) < k\}$ , ce qui a du sens pour les mêmes raisons. On construit en itérant ce procédé  $\varphi(n)$  tel que :

$$\forall n \in \mathbb{N}, \varphi(n+1) = \min\{k \in \mathbb{N} \mid |u_k - \ell| > \varepsilon, \varphi(n) < k\}.$$

De cette manière, nous venons de construire une extractrice telle que :

$$\forall n \in \mathbb{N}, |u_{\varphi(n)} - \ell| > \varepsilon.$$

Par hypothèse  $u$  est bornée, donc il existe  $M \in \mathbb{R}_+$  tel que :

$$\forall n \in \mathbb{N}, |u_n| \leq M,$$

donc pour tout  $n$  dans  $\mathbb{N}$ ,  $|u_{\varphi(n)}| \leq M$ , donc  $(u_{\varphi(n)})_{n \in \mathbb{N}}$  est bornée.

Par le théorème de Bolzano-Weierstrass, il existe  $\psi$  une extractrice et  $\ell' \in \mathbb{R}$ , avec  $\varphi \circ \psi$  qui est



aussi une extractrice par composition d'applications strictement croissantes, donc  $(u_{\varphi \circ \psi(n)})_{n \in \mathbb{N}}$  est une sous-suite de  $u$  et  $\ell' \in L(u) = \{\ell\}$ .  
Par ailleurs, pour tout  $n$  dans  $\mathbb{N}$  :

$$\underbrace{|u_{\varphi \circ \psi(n)} - \ell|}_{\xrightarrow[n \rightarrow +\infty]{} |\ell' - \ell|} > \varepsilon,$$

donc en passant à la limite dans l'inégalité on a pour tout  $n$  dans  $\mathbb{N}$ ,  $|\ell' - \ell| \geq \varepsilon > 0$ , ce qui n'est pas possible car  $\ell$  est la seule valeur d'adhérence possible et ici la différence n'est pas nulle.  $\square$

## 12 Semaine 12

### 12.1 Résolution d'une relation de récurrence linéaire d'ordre 1 à coefficients constants et avec second membre

Soient  $a \in \mathbb{K}$  et  $v \in \mathbb{K}^{\mathbb{N}}$  où  $\mathbb{K}$  peut être  $\mathbb{C}$  ou  $\mathbb{R}$ . L'ensemble des solutions de l'équation  $\forall n \in \mathbb{N}, u_{n+1} = au_n + v_n$  est la droite affine :

$$\{w + \lambda (a^n)_{n \in \mathbb{N}} \mid \lambda \in \mathbb{K}\} \quad (13)$$

*Démonstration.* Posons  $w$  la suite définie par

$$\begin{cases} w_0 = 1 \\ \forall n \in \mathbb{N}, w_{n+1} = aw_n + v_n \end{cases}$$

$w$  est "évidemment" solution de particulière de l'équation"

Maintenant que nous disposons d'une solution particulière, et ayant observé que l'équation est linéaire, mettons en œuvre l'artillerie classique pour exprimer l'ensemble des solutions par l'habituelle technique.

$$\begin{aligned} \forall n \in \mathbb{N}, u_{n+1} = au_n + v_n &\iff \forall n \in \mathbb{N}, u_{n+1} - au_n = v_n \\ &\iff \forall n \in \mathbb{N}, u_{n+1} - au_n = w_{n+1} - aw_n \\ &\iff \forall n \in \mathbb{N}, (u - w)_{n+1} = a(u - w)_n \\ &\iff u - w \in \text{Vect} \{(a^n)_{n \in \mathbb{N}}\} \\ &\iff \exists \lambda \in \mathbb{K} : u - w = \lambda (a^n)_{n \in \mathbb{N}} \\ &\iff \exists \lambda \in \mathbb{K} : \forall n \in \mathbb{N}, u_n = w_n + \lambda a^n \\ &\iff u \in \{(w_n + \lambda a^n)_{n \in \mathbb{N}} \mid \lambda \in \mathbb{K}\} \end{aligned}$$

□

### 12.2 Résolution d'une relation de récurrence linéaire homogène d'ordre 2 à coefficients constants dans $\mathbb{C}$ lorsque l'équation caractéristique possède un discriminant non nul

Soient  $(a, b) \in \mathbb{C}^2$ . L'ensemble des solutions  $S_H$  de l'équation d'inconnue  $u \in \mathbb{C}^{\mathbb{N}}$

$$\forall n \in \mathbb{N}, u_{n+2} = au_{n+1} + bu_n \quad (14)$$

est le plan vectoriel  $\text{Vect}\{(r_1^n)_{n \in \mathbb{N}}, (r_2^n)_{n \in \mathbb{N}}\}$  où  $r_1$  et  $r_2$  sont les racines de l'équation caractéristique ( $r^2 = ar + b$ ) quand  $\Delta \neq 0$ .

*Démonstration.* Soient  $(a, b) \in \mathbb{C}^2$  fq.

Lemme Soit  $r \in \mathbb{C}$ .  $(r^n)_{n \in \mathbb{N}}$  est solution de l'équation de récurrence si et seulement si  $r^2 = ar + b$ .

$$\begin{aligned} (r^n)_{n \in \mathbb{N}} \text{ est solution} &\iff \forall n \in \mathbb{N}, r^{n+2} = ar^{n+1} + br^n \\ &\iff \forall n \in \mathbb{N}, r^n (r^2 - ar - b) = 0 \\ &\iff r^2 - ar - b = 0 \end{aligned}$$

En particulier pour  $n \leftarrow 0$

$$\iff r^2 = ar + b$$

Considérons le cas où l'équation  $r^2 = ar + b$  admet deux racines distinctes ( $\Delta \neq 0$ )  $r_1$  et  $r_2$ . D'après le lemme,  $(r_1^n)_{n \in \mathbb{N}}$  et  $(r_2^n)_{n \in \mathbb{N}}$  sont solutions. Par linéarité de l'équation, toute combinaison linéaire est solution de l'équation homogène. Donc  $\text{Vect}\{(r_1^n)_{n \in \mathbb{N}}, (r_2^n)_{n \in \mathbb{N}}\} \subset S_H$ .

Réciproquement, soit  $u \in S_H$  fq. Étudions le système à deux inconnues  $(\lambda, \mu) \in \mathbb{C}^2$  :

$$\begin{cases} \lambda r_1^0 + \mu r_2^0 = u_0 \\ \lambda r_1^1 + \mu r_2^1 = u_1 \end{cases} \iff \begin{cases} \lambda + \mu = u_0 \\ \lambda r_1 + \mu r_2 = u_1 \end{cases}$$

$\begin{vmatrix} 1 & 1 \\ r_1 & r_2 \end{vmatrix} = r_2 - r_1 \neq 0$  Donc d'après les formules de Cramer, ce système admet une unique solution.

Considérons le prédicat  $\mathcal{P}(\cdot)$  défini pour tout  $n \in \mathbb{N}$  par :

$$u_n = \lambda r_1^n + \mu r_2^n \text{ et } u_{n+1} = \lambda r_1^{n+1} + \mu r_2^{n+1}$$

- $\mathcal{P}(0)$  est vrai par construction de  $\lambda$  et  $\mu$ .
- Soit  $n \in \mathbb{N}$  fq tq  $\mathcal{P}(n)$  vrai. D'après  $\mathcal{P}(n)$ ,  $u_{n+1} = \lambda r_1^{n+1} + \mu r_2^{n+1}$ .

$$\begin{aligned} u_{n+2} &= a u_{n+1} + b u_n \\ &= a (\lambda r_1^{n+1} + \mu r_2^{n+1}) + b (\lambda r_1^n + \mu r_2^n) \quad \text{d'après } \mathcal{P}(n) \\ &= \lambda r_1^n (a r_1 + b) + \mu r_2^n (a r_2 + b) \\ &= \lambda r_1^{n+2} + \mu r_2^{n+2} \quad \text{car } r_1 \text{ et } r_2 \text{ sont racine de } r^2 = ar + b \end{aligned}$$

Ainsi  $S_H \subset \text{Vect}\{(r_1^n)_{n \in \mathbb{N}}, (r_2^n)_{n \in \mathbb{N}}\}$ .

Par double inclusion,  $S_H = \text{Vect}\{(r_1^n)_{n \in \mathbb{N}}, (r_2^n)_{n \in \mathbb{N}}\}$ . □

### 12.3 Caractérisation de la convergence par l'unicité d'une valeur d'adhérence pour une suite bornée.

Soit  $u$  une suite bornée.  $u$  converge si et seulement si il existe  $\ell \in \mathbb{K}$  tel que  $L(u)$  est le singleton  $\ell$

*Démonstration.* Traitons le cas réel, celui sur  $\mathbb{C}$  est à adapter sans peine.

Supposons que  $u$  converge et posons  $\lim u = \ell \in \mathbb{R}$ . Toutes les sous-suites de  $u$  convergent vers  $\ell$  donc  $L(u) = \{\ell\}$ .

Supposons maintenant qu'il existe un unique  $\ell \in \mathbb{R}$  tel que  $L(u) = \{\ell\}$ . Par l'absurde, supposons que  $u$  ne converge pas vers  $\ell$ , c'est-à-dire :

$$\exists \varepsilon \in \mathbb{R}_+^* : \forall N \in \mathbb{N}, \exists n \in \mathbb{N} : n \geq N \text{ et } |u_n - \ell| > \varepsilon.$$

Fixons un tel  $\varepsilon$ .

Posons  $\varphi(0) = \min \{k \in \mathbb{N} \mid |u_k - \ell| > \varepsilon\}$ , ce qui a du sens car c'est une partie non-vide de  $\mathbb{N}$ . Posons ensuite  $\varphi(1) = \min \{k \in \mathbb{N} \mid |u_k - \ell| > \varepsilon, \varphi(0) < k\}$ , ce qui a du sens pour les mêmes raisons. On construit en itérant ce procédé  $\varphi(n)$  tel que :

$$\forall n \in \mathbb{N}, \varphi(n+1) = \min \{k \in \mathbb{N} \mid |u_k - \ell| > \varepsilon, \varphi(n) < k\}.$$

De cette manière, nous venons de construire une extractrice telle que :

$$\forall n \in \mathbb{N}, |u_{\varphi(n)} - \ell| > \varepsilon.$$

Par hypothèse  $u$  est bornée, donc il existe  $M \in \mathbb{R}_+$  tel que :

$$\forall n \in \mathbb{N}, |u_n| \leq M,$$

donc pour tout  $n$  dans  $\mathbb{N}$ ,  $|u_{\varphi(n)}| \leq M$ , donc  $(u_{\varphi(n)})_{n \in \mathbb{N}}$  est bornée.

Par le théorème de Bolzano-Weierstrass, il existe  $\psi$  une extractrice et  $\ell' \in \mathbb{R}$ , avec  $\varphi \circ \psi$  qui est aussi une extractrice par composition d'applications strictement croissantes, donc  $(u_{\varphi \circ \psi(n)})_{n \in \mathbb{N}}$  est une sous-suite de  $u$  et  $\ell' \in L(u) = \{\ell\}$ .

Par ailleurs, pour tout  $n$  dans  $\mathbb{N}$  :

$$\underbrace{|u_{\varphi \circ \psi(n)} - \ell|}_{\xrightarrow{n \rightarrow +\infty} |\ell' - \ell|} > \varepsilon,$$

donc en passant à la limite dans l'inégalité on a pour tout  $n$  dans  $\mathbb{N}$ ,  $|\ell' - \ell| \geq \varepsilon > 0$ , ce qui n'est pas possible car  $\ell$  est la seule valeur d'adhérence possible et ici la différence n'est pas nulle. □

## 12.4 Monotonie de $u$ et des sous-suites des termes pairs et impairs de la suite $u_{n+1} = f(u_n)$ selon la monotonie de $f$

Soient  $f : \mathcal{D} \rightarrow \mathbb{R}$  et  $I \subset \mathcal{D}_f$  une intervalle  $f$ -stable.

Soit  $(u_n)_{n \in \mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$  la suite récurrente associée à la fonction  $f$  c'est-à-dire  $\forall n \in \mathbb{N}, u_{n+1} = f(u_n)$ .

— Si  $f$  est croissante sur  $I$ .

Si  $u_1 \geq u_0$  alors  $u$  est croissante.

Si  $u_1 \leq u_0$  alors  $u$  est décroissante.

— Si  $f$  est décroissante sur  $I$ .

Les sous-suites  $(u_{2n})_{n \in \mathbb{N}}$  et  $(u_{2n+1})_{n \in \mathbb{N}}$  sont monotone et ont une monotonie opposée (utiliser les premiers termes pour trouver leur monotonie respectives).

*Démonstration.* Soient de tels  $f, I$  et  $u$ .

— Supposons que  $f$  est croissante sur  $I$ .

Supposons  $u_1 \geq u_0$ . Considérons le prédicat  $\mathcal{P}(\cdot)$  défini pour tout  $n \in \mathbb{N}$  par

$$\mathcal{P}(n) : "u_{n+1} \geq u_n"$$

Par hypothèse,  $u_1 \geq u_0$  donc  $\mathcal{P}(0)$  est vrai.

Soit  $n \in \mathbb{N}$  fq tq  $\mathcal{P}(n)$  vrai.

$$u_{n+1} \geq u_n \quad \underbrace{\implies}_{f \text{ est croissante sur } I} \quad f(u_{n+1}) \geq f(u_n) \implies u_{n+2} \geq u_{n+1}$$

Donc  $\mathcal{P}(n+1)$  est vrai.

Si  $u_1 \leq u_0$ , il suffit de changer  $\geq$  par  $\leq$  dans la récurrence ci-dessus.

— Supposons que  $f$  est décroissante sur  $I$ .

Donc  $\forall n \in \mathbb{N}, u_{2(n+1)} = f \circ f(u_{2n})$  et  $u_{2(n+1)+1} = f \circ f(u_{2n+1})$ . Or  $f \circ f$  est croissante, donc  $(u_{2n})_{n \in \mathbb{N}}$  et  $(u_{2n+1})_{n \in \mathbb{N}}$  sont monotones.

Supposons que  $(u_{2n})_{n \in \mathbb{N}}$  est croissante. Soit  $n \in \mathbb{N}$  fq. Alors

$$u_{2n} \leq u_{2(n+1)} \quad \underbrace{\implies}_{f \text{ est décroissante sur } I} \quad f(u_{2n}) \geq f(u_{2(n+1)}) \implies u_{2n+1} \geq u_{2(n+1)+1}$$

Donc  $(u_{2n+1})_{n \in \mathbb{N}}$  est décroissante.

De même, si  $(u_{2n})_{n \in \mathbb{N}}$  est décroissante alors  $(u_{2n+1})_{n \in \mathbb{N}}$  est croissante.

□

## 12.5 L'intérieur de l'ensemble des rationnels est vide.

Montrons que :  $\overset{\circ}{\mathbb{Q}} = \emptyset$

*Démonstration.* Par l'absurde, supposons que  $\mathbb{Q}$  possède au moins un point intérieur.

Fixons  $r_0 \in \overset{\circ}{\mathbb{Q}}$ . Par définition d'un point intérieur, il existe  $\varepsilon \in \mathbb{R}_+^* : ]r_0 - \varepsilon, r_0 + \varepsilon[ \subset \mathbb{Q}$ . Or, par densité des irrationnels dans  $\mathbb{R}$ , il existe  $\alpha \in \mathbb{R} \setminus \mathbb{Q} : r_0 - \varepsilon < \alpha < r_0 + \varepsilon$ . On en déduit que  $\alpha \in ]r_0 - \varepsilon, r_0 + \varepsilon[$ , or  $]r_0 - \varepsilon, r_0 + \varepsilon[ \subset \mathbb{Q}$  donc  $\alpha \in \mathbb{Q}$  ce qui contredit le choix de  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ . Ainsi,  $\overset{\circ}{\mathbb{Q}} = \emptyset$

□

## 12.6 Théorème sans nom version continue au voisinage de $a$

Soient  $f, g : \mathcal{D} \rightarrow \mathbb{R}$ ,  $\ell \in \mathbb{R}$  et  $a \in \overline{\mathcal{D}}$  tels que  $|f(x) - \ell| \leq g(x)$  au voisinage de  $a$  et  $g$  tend vers 0 en  $a$ . Alors  $f$  tend vers  $\ell$  en  $a$ .

*Démonstration.* On traite le cas  $a \in \mathbb{R}$ . Par définition de  $|f(x) - \ell| \leq g(x)$  au voisinage de  $a$ ,

$$\exists \eta \in \mathbb{R}_+^* : \forall x \in \mathcal{D}, |x - a| \leq \eta \implies |f(x) - \ell| \leq g(x).$$

Fixons un tel  $\eta$ .

Soit  $\omega \in \mathbb{R}_+^*$ . Appliquons la définition de  $\lim_{x \rightarrow a} g(x) = 0$  pour  $\varepsilon \leftarrow \omega$  :

$$\exists \eta' \in \mathbb{R}_+^* : \forall x \in \mathcal{D}, |x - a| \leq \eta' \implies |g(x)| \leq \omega.$$

Fixons un tel  $\eta'$ .

Posons  $\Omega = \min \{\eta, \eta'\}$ .

Soit  $x \in \mathcal{D}$  tel que  $|x - a| \leq \Omega$ .

$$|f(x) - \ell| \leq g(x) \leq \omega,$$

car la définition de  $\Omega$  permet de remplir les conditions des deux propriétés. □

## 13 Semaine 13

### 13.1 Théorème de composition des limites

Soient  $g$  une fonction définie sur  $\mathcal{D}_g \subset \mathbb{R}$  et  $f$  une fonction définie sur  $\mathcal{D}_f \subset \mathbb{R}$  telle que  $f(\mathcal{D}_f) \subset \mathcal{D}_g$ .

Si  $\left. \begin{array}{l} g \text{ admet une limite } \ell \in \overline{\mathbb{R}} \text{ en } b \in \overline{\mathcal{D}_g} \\ f \text{ admet } b \text{ comme limite en } a \in \mathcal{D}_f \end{array} \right\}$  alors  $g \circ f$  admet  $\ell$  comme limite en  $a$ .

*Démonstration.* Traitons le cas où  $\ell \in \mathbb{R}$ ,  $a \in \mathbb{R}$  et  $b \in \mathbb{R}$ .

Soit  $\varepsilon \in \mathbb{R}_+^*$  fq.

Appliquons la définition de  $g(y) \xrightarrow{y \rightarrow b} \ell$  pour cet  $\varepsilon$  :

$$\exists \eta_g \in \mathbb{R}_+^* : \forall y \in \mathcal{D}_g, |y - b| \leq \eta_g \implies |g(y) - \ell| \leq \varepsilon$$

Appliquons la définition de  $f(x) \xrightarrow{x \rightarrow a} b$  pour cet  $\eta_g$  :

$$\exists \eta_f \in \mathbb{R}_+^* : \forall x \in \mathcal{D}_f, |x - a| \leq \eta_f \implies |f(x) - b| \leq \eta_g$$

Posons  $\eta = \eta_f$ .

Soit  $x \in \mathcal{D}_{g \circ f}$  fq tq  $|x - a| \leq \eta$ . Or  $f(\mathcal{D}_f) \subset \mathcal{D}_g$  donc  $\mathcal{D}_{g \circ f} = \mathcal{D}_f$ .

Ainsi,  $x \in \mathcal{D}_f$  et  $|x - a| \leq \eta_f$  d'où  $|f(x) - b| \leq \eta_g$  d'où  $|g(f(x)) - \ell| \leq \varepsilon$ . Donc

$$g \circ f \xrightarrow{x \rightarrow a} \ell$$

□

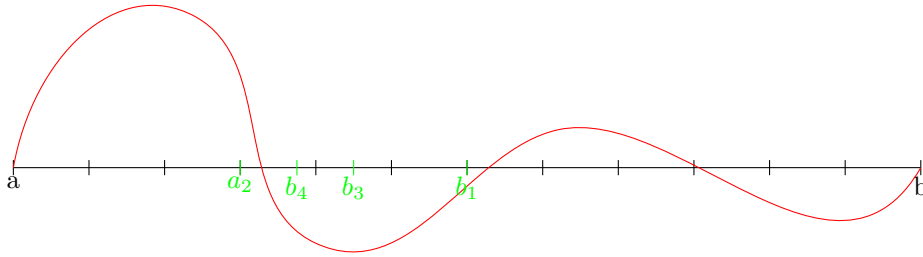
### 13.2 Théorème des valeurs intermédiaires

Soit une fonction continue  $f : [a; b] \rightarrow \mathbb{R}$  avec  $(a, b) \in \mathbb{R}^2$  et  $a < b$ .

Si  $f(a)f(b) \leq 0$  alors  $\exists c \in [a; b] : f(c) = 0$ .

On rencontre aussi : Si  $f(a)f(b) < 0$  alors  $\exists c \in ]a; b[ : f(c) = 0$ .

*Démonstration.* La démonstration repose sur la technique de la dichotomie.



Soient  $a, b, f$  de tels objets. Procédons à la construction des suites  $(a_n)_{n \in \mathbb{N}}, (b_n)_{n \in \mathbb{N}}, (c_n)_{n \in \mathbb{N}}$ .

Posons  $a_0 = a$ ,  $b_0 = b$  et  $c_0 = \frac{a+b}{2}$  (le milieu du segment  $[a; b]$ ). Nous avons, par hypothèse  $f(a_0)f(b_0) \leq 0$ .

Soit  $n \in \mathbb{N}$  fq. Supposons les trois suites construites au rang  $n$  telles que  $f(a_n)f(b_n) \leq 0$  et  $c_n = \frac{a_n+b_n}{2}$  (milieu de  $[a_n; b_n]$ ).

— Si  $f(a_n)f(b_n) \leq 0$ , posons  $\left| \begin{array}{lcl} a_{n+1} & = & a_n \\ b_{n+1} & = & c_n \\ c_{n+1} & = & \frac{a_{n+1}+b_{n+1}}{2} \end{array} \right.$

— Sinon  $f(a_n)f(b_n) > 0$ . Or  $f(a_n)f(b_n) \leq 0$ , donc  $f(a_n)^2 f(b_n)f(c_n) \leq 0$ . Donc  $f(b_n)f(c_n) \leq 0$ .

Posons  $\left| \begin{array}{lcl} a_{n+1} & = & c_n \\ b_{n+1} & = & b_n \\ c_{n+1} & = & \frac{a_{n+1}+b_{n+1}}{2} \end{array} \right.$

Ainsi, nous avons bien construits  $a_{n+1}, b_{n+1}, c_{n+1}$  telles que  $f(a_{n+1})f(b_{n+1}) \leq 0$  et  $c_{n+1} = \frac{a_{n+1}+b_{n+1}}{2}$  (milieu de  $[a_{n+1}; b_{n+1}]$ ).

Par récurrence immédiate,  $(a_n)_{n \in \mathbb{N}}$  est croissante,  $(b_n)_{n \in \mathbb{N}}$  est décroissante et  $\forall n \in \mathbb{N}, b_n - a_n = \frac{b-a}{2^n}$  d'où  $b_n - a_n \xrightarrow{n \rightarrow +\infty} 0$ . Donc les suites  $a$  et  $b$  sont adjacentes. D'après le théorème des suites adjacentes, elles convergent vers la même limite. Notons la  $c$ .

D'après le bonus de ce même théorème,  $\forall n \in \mathbb{N}, a_n \leq c \leq b_n$  donc pour  $n = 0$ ,  $a \leq c \leq b$ . Ainsi,

$$c \in [a; b]$$

Par ailleurs,  $\forall n \in \mathbb{N}, f(a_n)f(b_n) \leq 0$ . Par continuité de  $f$  sur  $[a; b]$  donc en  $c$ ,  $f(a_n) \xrightarrow{n \rightarrow +\infty} f(c)$  et  $f(b_n) \xrightarrow{n \rightarrow +\infty} f(c)$ . Par passage à limite dans l'inégalité,

$$f(c) \times f(c) \leq 0$$

Or  $f(c)^2 \geq 0$ , d'où  $f(c)^2 = 0$ . Ainsi,

$$f(c) = 0$$

Donc  $c$  est un point fixe. □

### 13.3 Théorème de Weierstraß

L'image d'un segment par une fonction continue sur ce segment est un segment : soient  $(a, b) \in \mathbb{R}^2$  tels que  $a < b$  et  $f : [a, b] \rightarrow \mathbb{R}$ . Si  $f \in C^0([a, b], \mathbb{R})$  alors  $\exists (x_1, x_2) \in \mathbb{R}^2 : f([a, b]) = [f(x_1), f(x_2)]$

*Démonstration.* — *Étape 1* Montrons que  $f([a, b])$  est majoré.

Par l'absurde, supposons que  $f([a, b])$  n'est pas majoré

Alors

$$\forall A \in \mathbb{R}, \exists x \in [a, b] : f(x) > A \quad (15)$$

Soit  $n \in \mathbb{N}$  fq. Appliquons (15) pour  $A \leftarrow n : \exists x \in [a, b] : f(x) > n$ , et fixons un tel  $x$  que l'on note  $x_n$ . Nous venons de créer la suite  $(x_n)_{n \in \mathbb{N}} \in [a, b]^{\mathbb{N}}$  qui vérifie :

$$\left\{ \begin{array}{l} \forall n \in \mathbb{N}, f(x_n) \geq n \\ \lim_{n \rightarrow \infty} n = +\infty \end{array} \right\} \xRightarrow{\text{théorème de divergence par minoration}} f(x_n) \xrightarrow{n \rightarrow +\infty} +\infty$$

$(x_n)_{n \in \mathbb{N}}$  est bornée (à valeurs dans  $[a, b]$ ) donc, selon le théorème de Bolzano-Weierstraß :

$$\exists \ell \in \mathbb{R} : \exists \varphi : \mathbb{N} \rightarrow \mathbb{N} : \text{strict. croissante tel que } (x_{\varphi(n)})_{n \in \mathbb{N}} \text{ tend vers } \ell$$

Donc, en passant à la limite :  $\forall n \in \mathbb{N}, a \leq x_{\varphi(n)} \leq b \implies a \leq \ell \leq b \implies \ell \in [a, b]$

Par continuité de  $f$  sur  $[a, b]$ , donc en  $\ell$ ,  $(f(x_{\varphi(n)}))_{n \in \mathbb{N}}$  converge vers  $f(\ell)$ .

Or

$$\left\{ \begin{array}{l} (f(x_{\varphi(n)}))_{n \in \mathbb{N}} \text{ est une sous suite de } (f(x_n))_{n \in \mathbb{N}} \\ f(x_n) \xrightarrow{n \rightarrow +\infty} +\infty \end{array} \right.$$

donc  $(f(x_{\varphi(n)}))_{n \in \mathbb{N}}$ , tend vers  $+\infty$ , ce qui est absurde, donc  $f$  est majorée.

On fait de même pour la minoration.

— *Étape 2* : Montrons que  $f([a, b])$  admet un pge et un ppe.

Montrons donc que  $f([a, b])$  admet une borne sup, qui, puisque c'est une valeur atteinte, deviendra un max.

$$f([a, b]) \text{ est } \left\{ \begin{array}{l} \text{une partie de } \mathbb{R} \\ \text{non vide car contient } f(a) \\ \text{majorée d'après l'étape 1} \end{array} \right.$$

$f([a, b])$  admet donc une borne supérieure  $\sigma$ .

Appliquons la caractérisation séquentielle de la borne supérieure :

$$\exists (y_n)_{n \in \mathbb{N}}, \in f([a, b])^{\mathbb{N}} : (y_n) \text{ converge vers } \sigma$$

$$\forall n \in \mathbb{N}, y_n \in f([a, b]) \implies \exists x_n \in [a, b] : f(x_n) = y_n$$

Fixons un tel  $x_n$  pour tout  $y_n$ . On a donc construit  $(x_n)_{n \in \mathbb{N}} \in [a, b]^{\mathbb{N}} : f(x_n) \xrightarrow[n \rightarrow +\infty]{} \sigma$

De plus,  $(x_n)$  est bornée (à valeurs dans  $[a, b]$ ) donc, selon le théorème de Bolzano-Weierstraß :

$$\exists \ell \in \mathbb{R} : \exists \varphi : \mathbb{N} \rightarrow \mathbb{N} \text{ strict. croissante tel que } (x_{\varphi(n)})_{n \in \mathbb{N}} \text{ tend vers } \ell$$

Donc, en passant à la limite :  $\forall n \in \mathbb{N}, a \leq x_{\varphi(n)} \leq b \implies a \leq \ell \leq b \implies \ell \in [a, b]$

Par continuité de  $f$  sur  $[a, b]$ , donc en  $\ell$ ,  $(f(x_{\varphi(n)}))_{n \in \mathbb{N}}$  converge vers  $f(\ell)$ .

Or,

$$\left\{ \begin{array}{l} (f(x_{\varphi(n)}))_{n \in \mathbb{N}} \text{ est une sous suite de } (f(x_n))_{n \in \mathbb{N}} \\ f(x_n) \xrightarrow[n \rightarrow +\infty]{} \sigma \end{array} \right.$$

Par unicité de la limite,  $\sigma = f(\ell)$ .

On montre de même qu'il existe  $\ell' \in [a, b] : f(\ell') = \inf f([a, b])$

Ainsi,  $f(\ell) = \max f([a, b])$  et  $f(\ell') = \min f([a, b])$

— *Étape 3* : Montrons que  $f([a, b]) = [f(\ell'), f(\ell)]$ .

Par la construction précédente,  $\forall y \in f([a, b]), y \in [f(\ell'), f(\ell)]$ .

Ainsi,  $f([a, b]) \subset [f(\ell'), f(\ell)]$ .

Réciproquement, l'image par la fonction continue  $f$  du segment  $[a, b]$  qui est un intervalle est un intervalle :

$$\left. \begin{array}{l} f([a, b]) \text{ est un intervalle} \\ f(\ell) \in f([a, b]) \\ f(\ell') \in f([a, b]) \end{array} \right\} \implies [f(\ell'), f(\ell)] \subset f([a, b])$$

D'où  $[f(\ell'), f(\ell)] = f([a, b])$

□



## 14 Semaine 14

### 14.1 Expression de dérivées successives

Soit  $f \left| \begin{array}{l} \mathbb{R}_+^* \rightarrow \mathbb{R} \\ x \mapsto \frac{\ln x}{x} \end{array} \right.$ .

Exprimer  $f^{(n)}$  pour tout  $n \in \mathbb{N}$ .

*Démonstration.* Soit  $x \in \mathcal{D}_f$ .

Considérons le prédicat  $P(\cdot)$  définit pour  $n \in \mathbb{N}$  par :

$$P(n) : " f^{(n)}(x) = \frac{(-1)^n n!}{x^{n+1}} \left[ \ln(x) - \sum_{k=1}^n \frac{1}{k} \right] "$$

Initialisation :

Pour  $n = 0$ ,

$$f^{(0)}(x) = f(x) = \frac{\ln(x)}{x} = \frac{(-1)^0 0!}{x^{0+1}} \left[ \ln(x) - \sum_{k=1}^0 \frac{1}{k} \right],$$

donc  $P(0)$  est vrai.

Hérédité :

Soit  $n \in \mathbb{N}$  tel que  $P(n)$ . On a,

$$f^{(n+1)}(x) = (f^{(n)}(x))' = \left( \frac{(-1)^n n!}{x^{n+1}} \left[ \ln(x) - \sum_{k=1}^n \frac{1}{k} \right] \right)'$$

par véracité de  $P(n)$ . Ainsi,

$$\begin{aligned} f^{(n+1)}(x) &= \frac{(-1)^n n! x^n - (-1)^n (n+1)! x^n [\ln(x) - \sum_{k=1}^n \frac{1}{k}]}{x^{2(n+1)}} \\ &= \frac{(-1)^{n+1} (n+1)! \ln(x) - (-1)^{n+1} (n+1)! \sum_{k=1}^{n+1} \frac{1}{k}}{x^{n+2}} \\ &= \frac{(-1)^{n+1} (n+1)!}{x^{n+2}} \left[ \ln(x) - \sum_{k=1}^{n+1} \frac{1}{k} \right] \end{aligned}$$

c'est l'expression recherchée, donc  $P(n+1)$  est vrai.

Par théorème de récurrence sur  $\mathbb{N}$ ,  $P(n)$  est vraie pour tout  $n \in \mathbb{N}$ . □

### 14.2 Dérivé d'une bijection réciproque

Soit  $f : I \rightarrow f(I) \subset \mathbb{R}$  continue, strictement monotone sur  $I$  et dérivable en  $a \in I$ . Si  $f'(a) \neq 0$  alors  $f$  est bijective,  $f^{-1}$  est dérivable en  $f(a)$  et  $f^{-1}(f(a)) = \frac{1}{f'(a)}$ .

*Démonstration.* Soient de tels objets.

Rappelons le lemme inattendu. Soit  $g : J \rightarrow \mathbb{R}$  monotone (où  $J$  est un intervalle). Nous avons l'équivalence suivante :

$$f(J) \text{ est un intervalle} \iff f \text{ est continue sur } J$$

Par définition,  $f$  est surjective. Comme elle est strictement monotone,  $f$  est injective. Ainsi  $f$  est bijective.

D'après le lemme inattendu,  $f(I)$  est un intervalle. Nous avons  $f^{-1} : f(I) \rightarrow I$  avec  $f(I)$  et  $I$  des intervalles donc  $f^{-1}$  est continue sur  $f(I)$ .

Calculons la limite du taux d'accroissement de  $f^{-1}$  en  $f(a)$  :

$$\forall x \in f(I), \tau_{f^{-1}, f(a)} = \frac{f^{-1}(x) - f^{-1}(f(a))}{x - f(a)}$$

Posons  $u = f^{-1}(x)$ . D'où :

$$\tau_{f^{-1}, f(a)} = \frac{u - a}{f(u) - f(a)}$$

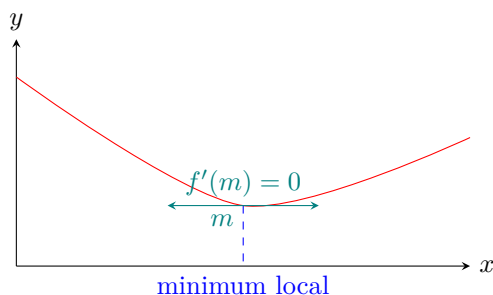
De plus, par continuité de  $f^{-1}$ ,  $u \xrightarrow{x \rightarrow f(a)} f^{-1}(f(a)) = a$ . Par dérivabilité en  $a$  et par continuité

de  $x \mapsto x^{-1}$  en  $f(a) \neq 0$ ,  $\frac{u-a}{f(u)-f(a)} \xrightarrow{u \rightarrow a} \frac{1}{f'(a)}$ .

Ainsi,  $f^{-1}$  est dérivable en  $f(a)$  et  $f^{-1}(f(a)) = \frac{1}{f'(a)}$ . □

### 14.3 Dérivée d'un extremum local intérieur au domaine de définition

Soit  $f : I \rightarrow \mathbb{R}$ . Si  $f$  admet un extremum local en  $a \in \overset{\circ}{I}$  et si  $f$  est dérivable en  $a$  alors  $f'(a) = 0$



*Démonstration.* Soient de tels objets.

$a \in \overset{\circ}{I} \implies \exists \eta_1 \in \mathbb{R}_+^* : [a - \eta_1; a + \eta_1] \subset I$  Fixons un tel  $\eta_1$ .

Calculons le taux d'accroissement en  $a$ .

$$\forall x \in [a - \eta_1; a + \eta_1], \tau_{f,a}(x) = \frac{f(x) - f(a)}{x - a}.$$

Or  $f$  est dérivable en  $a$  donc  $\tau_{f,a}(x)$  admet une limite lorsque  $x \rightarrow a$ . Traitons le cas où  $a$  est maximum local. Par définition :

$$\exists \eta_2 \in \mathbb{R}_+^* : \forall x \in [a - \eta_2; a + \eta_2], f(x) \leq f(a)$$

Fixons un tel  $\eta_2$ . Soit  $x \in [a - \eta_2; a + \eta_2] \setminus \{a\}$  fq.

Alors  $f(x) - f(a) \leq 0$ .

Si  $x > a$ ,  $x - a > 0$ . Alors  $\frac{f(x) - f(a)}{x - a} \leq 0$ . Donc  $\lim_{x \rightarrow a} \tau_{f,a}(x) \leq 0$ .

Sinon  $x < a$ ,  $x - a < 0$ . Alors  $\frac{f(x) - f(a)}{x - a} \geq 0$ . Donc  $\lim_{x \rightarrow a} \tau_{f,a}(x) \geq 0$ .

Ainsi  $0 \leq \lim_{x \rightarrow a} \tau_{f,a}(x) \leq 0$ . Donc  $f'(a) = 0$ . □

### 14.4 Théorème de Rolle et formule des accroissements finis

Soient  $(a, b) \in \mathbb{R}^2$  tels que  $a < b$ . Soit  $I$  le segment  $a, b$ .

Soit  $f : I \rightarrow \mathbb{R}$  continue sur ledit segment et dérivable sur l'ouvert associé.

(i) Théorème de Rolle :

Si  $f(a) = f(b)$ , alors  $\exists c \in \overset{\circ}{I}$  tel que  $f'(c) = 0$

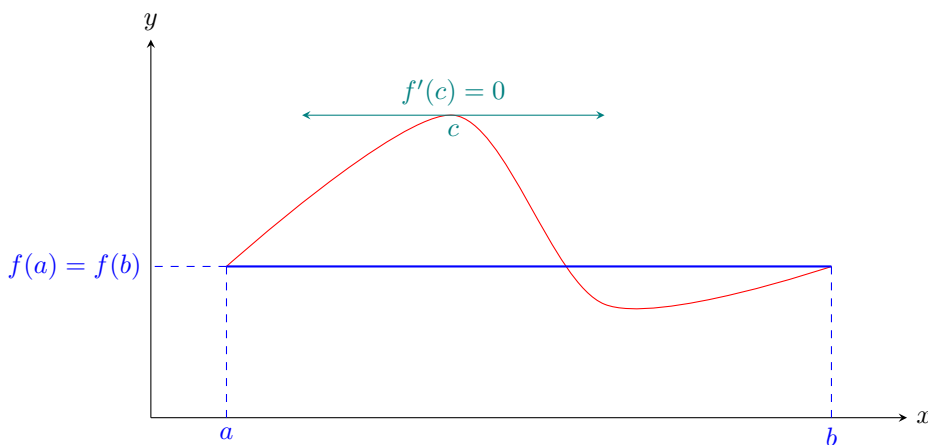


FIGURE 1 – Théorème de Rolle

(ii) Formule des accroissements finis :

$$\exists c \in \overset{\circ}{I} : f'(c) = \frac{f(b) - f(a)}{b - a}.$$

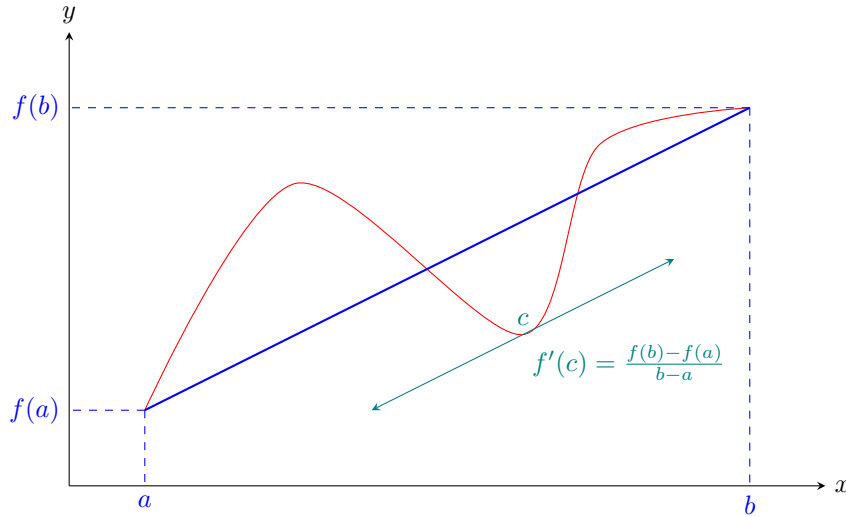


FIGURE 2 – Formule des accroissements finis

*Démonstration.* Soient de tels objets.

Prouvons (i), donc supposons  $f(a) = f(b)$ .

$f$  est continue sur  $I$  donc par le théorème de Weierstraß, elle est bornée et atteint ses bornes sur ce segment :

$$\exists (x_m, x_M) \in I^2 : (f(x_m) = \min f(I)) \wedge (f(x_M) = \max f(I))$$

donc, si  $(x_m, x_M) \in \{a, b\}^2$ , alors,

$$\forall x \in I, f(a) = f(x_m) \leq f(x) \leq f(x_M) = f(a)$$

donc  $\forall x \in I, f(x) = f(a)$  c'est-à-dire que  $f$  est constante et donc tous les points intermédiaires à  $I$  sont des  $c$  valides.

Sinon,  $(x_m \notin \{a, b\}) \vee (x_M \notin \{a, b\})$ , quitte à prendre l'autre valeur, supposons que  $x_M \notin \{a, b\}$ , ainsi,  $x_M \in \overset{\circ}{I}$  et  $f(x_M)$  est un maximum global donc,  $f$  étant dérivable sur  $\overset{\circ}{I}$  elle est dérivable en  $x_M$  donc  $f'(x_M) = 0$ , on pose  $c = x_M$ , ce qui conclut.

Prouvons (ii).

Posons  $d : I \rightarrow \mathbb{R}, x \mapsto f(x) - \left( \frac{f(b)-f(a)}{b-a}(x-a) + f(a) \right)$ .  $d$  est continue sur  $I$  et dérivable sur  $\overset{\circ}{I}$  comme combinaison linéaire de telles fonctions. On a  $d(a) = 0$  et  $d(b) = 0$  donc  $d(a) = 0 = d(b)$ .

On peut alors appliquer le Théorème de Rolle pour  $f \leftarrow d, a \leftarrow a$  et  $b \leftarrow b$  : il existe  $c \in \overset{\circ}{I}$  tel que  $d'(c) = 0$ , c'est le résultat.  $\square$

## 14.5 Inégalité des accroissements finis

Soit  $f \in \mathcal{C}^0(I, \mathbb{R}) \cap \mathcal{D}^1(\overset{\circ}{I}, \mathbb{R})$  et  $x_0 \in I$ , posons  $X_- = ]-\infty; x_0]$  la demi-droite fermée en  $x_0$  et vers  $-\infty$ , de même  $X_+ = [x_0; +\infty[$  la demi-droite fermée en  $x_0$  et vers  $+\infty$ .

(i) ★ Si  $\exists m \in \mathbb{R} : \forall x \in \overset{\circ}{I}, m \leq f'(x)$ , alors,

$$\forall x \in I \cap X_+, f(x_0) + m(x - x_0) \leq f(x)$$

et

$$\forall x \in I \cap X_-, f(x) \leq f(x_0) + m(x - x_0)$$

★ Si  $\exists M \in \mathbb{R} : \forall x \in \overset{\circ}{I}, f'(x) \leq M$ , alors,

$$\forall x \in I \cap X_+, f(x) \leq f(x_0) + M(x - x_0)$$

et

$$\forall x \in I \cap X_-, f(x_0) + M(x - x_0) \leq f(x)$$

★ Si  $\exists (m, M) \in \mathbb{R}^2 : \forall x \in \overset{\circ}{I}, m \leq f'(x) \leq M$ , alors,

$$\forall x \in I \cap X_+, f(x_0) + m(x - x_0) \leq f(x) \leq f(x_0) + M(x - x_0)$$

et

$$\forall x \in I \cap X_-, f(x_0) + M(x - x_0) \leq f(x) \leq f(x_0) + m(x - x_0)$$

(ii) Si  $\exists M \in \mathbb{R} : \forall x \in \overset{\circ}{I}, |f'(x)| \leq M$ , alors,

$$\forall (x, y) \in I^2, |f(y) - f(x)| \leq M|y - x|$$

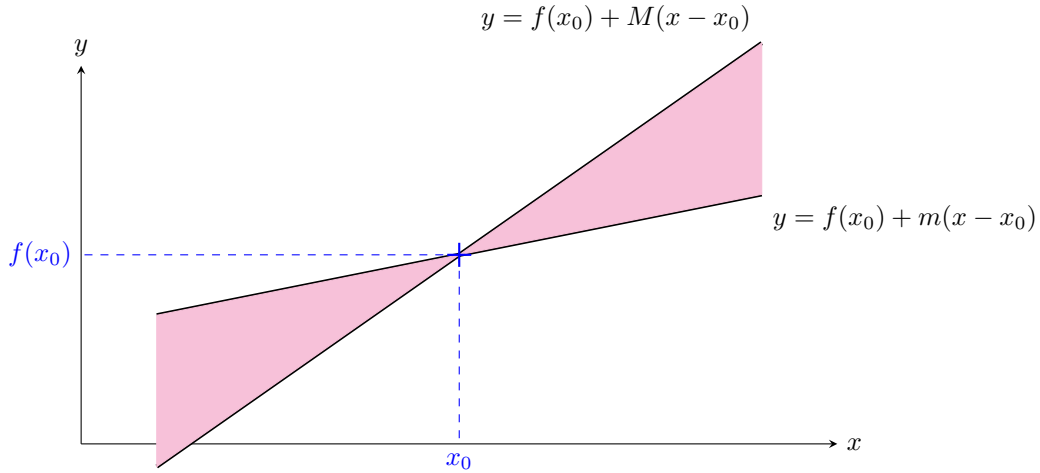


FIGURE 3 – Interprétation géométrique des accroissements finis

*Démonstration.* (i) Soit  $x \in I$  et posons  $S$  le segment d'extrémités  $x$  et  $x_0$ .

★ Si  $x \neq x_0$ ,  $f$  est continue sur  $S$  et dérivable sur  $\overset{\circ}{S}$ , la formule des accroissements finis donne alors l'existence d'un  $c$  appartenant à  $\overset{\circ}{S}$  tel que

$$f(x) - f(x_0) = (x - x_0)f'(c)$$

Si  $x > x_0$ ,  $x - x_0 > 0$ , or  $m \leq f'(c) \leq M$  donc

$$m(x - x_0) \leq (x - x_0)f'(c) \leq M(x - x_0)$$

si bien que

$$m(x - x_0) \leq f(x) - f(x_0) \leq M(x - x_0)$$

d'où

$$f(x_0) + m(x - x_0) \leq f(x) \leq f(x_0) + M(x - x_0).$$

Si  $x < x_0$ , il suffit de retourner l'inégalité lors de la première multiplication et (i) est prouvé.

(ii) Soit  $y \in I$ .

L'hypothèse  $\forall x \in \overset{\circ}{I}, |f'(x)| \leq M$  équivaut à  $\forall x \in \overset{\circ}{I}, -M \leq f'(x) \leq M$ , donc on peut appliquer (i) pour  $x_0 \leftarrow y$ ,  $M \leftarrow M$  et  $m \leftarrow -M$  :

$$\forall x \in I \cap [y, +\infty[, f(y) - M(x - y) \leq f(x) \leq f(y) + M(x - y)$$

Or  $x - y > 0$  donc  $|f(x) - f(y)| \leq M|x - y|$ . Et

$$\forall x \in I \cap ]-\infty, y], f(y) + M(x - y) \leq f(x) \leq f(y) - M(x - y)$$

Or  $x - y < 0$  donc  $|f(x) - f(y)| \leq M|x - y|$ .

Par conséquent,  $\forall (x, y) \in I^2, |f(y) - f(x)| \leq M|y - x|$ . □

## 14.6 Caractère lipschitzien d'une fonction $\mathcal{C}^1$ sur un segment

Soit  $f \in \mathcal{C}^1(I, \mathbb{R})$ ,  $I$  le segment  $a, b$ . Alors  $f$  est  $\|f'\|_{\infty, I}$ -lipschitzienne sur  $I$ .

*Démonstration.* Soient de tels objets.

★  $f \in \mathcal{C}^1(I, \mathbb{R})$  donc  $f \in \mathcal{C}^0(I, \mathbb{R})$ .

★  $f \in \mathcal{C}^1(I, \mathbb{R})$  donc  $f \in \mathcal{D}^1(\overset{\circ}{I}, \mathbb{R})$ .

★  $f \in \mathcal{C}^1(I, \mathbb{R})$  donc  $f'$  est continue sur  $I$  donc le réel  $\|f'\|_{\infty, I}$  est bien défini et

$$\forall x \in \overset{\circ}{I}, |f'(x)| \leq \|f'\|_{\infty, I}.$$

Ces propriétés permettent d'appliquer le corollaire du TAF qui conclut que  $f$  est  $\|f'\|_{\infty, I}$ -lipschitzienne.  $\square$

## 14.7 Théorème du prolongement de la propriété de la dérivabilité

Soit  $f \in \mathcal{F}(I, \mathbb{R})$  et  $a \in I$ .

*Lemme :*

Si  $\left\{ \begin{array}{l} f \text{ est dérivable sur } I \setminus \{a\} \\ f \text{ est continue en } a \\ f'_{|I \setminus \{a\}} \text{ admet une limite } \ell \in \overline{\mathbb{R}} \text{ en } a \end{array} \right. , \text{ alors } \lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a} = \ell$

*Théorème :*

Si  $\left\{ \begin{array}{l} f \text{ est dérivable sur } I \setminus \{a\} \\ f \text{ est continue en } a \\ f'_{|I \setminus \{a\}} \text{ admet une limite finie } \ell \in \mathbb{R} \text{ en } a \end{array} \right. , \text{ alors } \left\{ \begin{array}{l} f \text{ est dérivable en } a \\ f'(a) = \ell \text{ (donc } f' \text{ est continue en } a) \end{array} \right.$

*Démonstration.* Prouvons le lemme pour  $\ell \in \mathbb{R}$ , c'est le cas qui nous intéresse.

Soient de tels objets. Soit  $\varepsilon \in \mathbb{R}_+^*$ . Appliquons la définition de  $\lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a} = \ell$  pour  $\varepsilon \leftarrow \varepsilon$  :

$$\exists \eta \in \mathbb{R}_+^* : \forall x \in I \setminus \{a\}, |x - a| \leq \eta \implies |f'_{|I \setminus \{a\}}(x) - \ell| \leq \varepsilon.$$

Fixons un tel  $\eta$ .

Soit  $x \in I \setminus \{a\}$  tel que  $|x - a| \leq \eta$ .

La fonction  $f$  est continue sur  $I$  donc  $f$  est continue sur le segment d'extrémités  $a$  et  $x$  qui est par ailleurs inclus dans  $I$  par convexité d'un intervalle.

La fonction  $f$  est dérivable sur  $I$  donc  $f$  est dérivable sur l'intervalle ouvert  $a, x$  qui est aussi inclus dans  $\overset{\circ}{I}$  par convexité.

L'égalité des accroissements finis s'applique à  $f$  sur l'intervalle  $a$  et  $x$  :

$$\exists c_x \in ]a, x[ \cup ]x, a[ : \frac{f(x) - f(a)}{x - a} = f'(c_x)$$

Or  $|c_x - a| \leq |x - a| \leq \eta$  donc ladite définition de la limite s'applique pour  $x \leftarrow c_x : |f'(c_x) - \ell| \leq \varepsilon$  si bien que

$$\left| \frac{f(x) - f(a)}{x - a} - \ell \right| \leq \varepsilon.$$

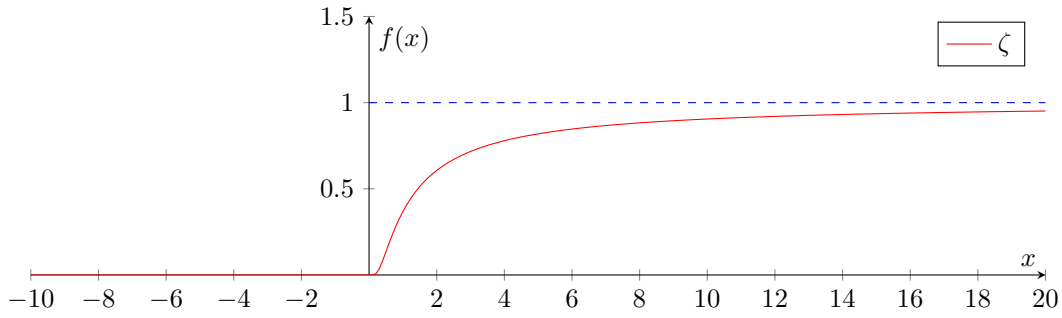
D'où le lemme.

Prouvons alors le théorème.

Sous ces hypothèses, le lemme s'applique donc  $\lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a} = \ell$ , or  $\ell \in \mathbb{R}$ , donc le taux d'accroissement de  $f$  en  $a$  admet une limite finie en  $a$  ce qui prouve la dérivabilité de  $f$  en  $a$  et  $f'(a) = \ell$ . Ce qui suffit.  $\square$

## 14.8 La fonction $\zeta$ (pas celle-là une autre) est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$

Posons  $\zeta \left| \begin{array}{l} \mathbb{R} \longrightarrow \mathbb{R} \\ x \mapsto \begin{cases} 0 & \text{si } x \leq 0 \\ e^{-\frac{1}{x}} & \text{si } x > 0 \end{cases} \end{array} \right. . \text{ Montrons que } \zeta \in \mathcal{C}^\infty(\mathbb{R}, \mathbb{R}).$



*Démonstration.*

- ★  $\zeta|_{]-\infty;0[}$  est constante donc  $\zeta \in \mathcal{C}^\infty(]-\infty;0[, \mathbb{R})$ .
- ★  $x \mapsto -\frac{1}{x} \in \mathcal{C}^\infty(]0;+\infty[, ]-\infty;0[)$  et  $\exp \in \mathcal{C}^\infty(]-\infty;0[, \mathbb{R})$  donc, par stabilité de  $\mathcal{C}^\infty$  par composition,  $\zeta \in \mathcal{C}^\infty(]0;+\infty[, \mathbb{R})$ .

Considérons le prédicat  $\mathcal{P}(\cdot)$  défini pour tout  $n \in \mathbb{N}$  :

$$\mathcal{P} : \text{“} \exists P_n \in \mathbb{R}[x] : \forall x \in \mathbb{R}^*, \zeta^{(n)} = \begin{cases} 0 & \text{si } x < 0 \\ \frac{P_n(x)}{x^{2n}} e^{-\frac{1}{x}} & \text{si } x > 0 \end{cases} \text{”} \quad (16)$$

- ★  $\mathcal{P}(0)$  est vrai par définition de  $\zeta$  en posant  $P_0(x) = 1$
- ★ Soit  $n \in \mathbb{N}^*$  fixé quelconque tel que  $\mathcal{P}$  est vrai. D'une part,  $\forall x \in ]-\infty;0[, \zeta^{(n)}(x) = 0$  donc

$$\forall x \in ]-\infty;0[, \zeta^{(n+1)}(x) = 0$$

D'autre part,  $\forall x \in ]0;+\infty[, \zeta^{(n)}(x) = \frac{P_n(x)}{x^{2n}} e^{-\frac{1}{x}}$  ce qui est un produit de trois expressions dérivables. D'où :

$$\begin{aligned} \forall x \in ]-\infty;0[, \zeta^{(n+1)}(x) &= \left( P'_n(x) \frac{1}{x^{2n}} + P_n(x) \frac{-2n}{x^{2n+1}} + \frac{P_n(x)}{x^{2n}} \frac{1}{x^2} \right) e^{-\frac{1}{x}} \\ &= \frac{x^2 P'_n(x) - 2nx P_n(x) + P_n(x)}{x^{2(n+1)}} e^{-\frac{1}{x}} \end{aligned}$$

Si bien qu'en posant  $P_{n+1}(x) = x^2 P'_n(x) - 2nx P_n(x) + P_n(x) \in \mathbb{R}[x]$ , on obtient :

$$\forall x \in ]0;+\infty[, \zeta^{(n+1)}(x) = \frac{P_{n+1}(x)}{x^{2(n+1)}} e^{-\frac{1}{x}}$$

Par conséquent,  $\mathcal{P}(x)$  est vrai.

Appliquons maintenant le théorème de prolongement du caractère  $\mathcal{C}^\infty$ .

- ★ Nous avons montré que  $\zeta \in \mathcal{C}^\infty(\mathbb{R} \setminus \{0\}, \mathbb{R})$ .
  - ★ Calculons les limites à gauche et à droite de 0. Soit  $k \in \mathbb{N}$  fixé quelconque.
    - ★★  $\zeta^{(k)}$  est nulle sur  $]-\infty;0[, \zeta^{(k)} \xrightarrow{x \rightarrow 0^-} 0$ .
    - ★★ De plus,  $\exists P_k \in \mathbb{R}[x] : \forall x \in ]0;+\infty[, \zeta^{(k)}(x) = \frac{P_k(x)}{x^{2k}} e^{-\frac{1}{x}}$ . Posons  $u = \frac{1}{x}$ , ainsi  $\zeta^{(k)}(x) = u^{2k} P_k(\frac{1}{u}) e^{-\frac{1}{x}}$  et  $u \xrightarrow{x \rightarrow 0^+} +\infty$ .
- Le théorème des croissances comparées donne  $u^{2k} P_k(\frac{1}{u}) e^{-u} \xrightarrow{u \rightarrow +\infty} 0$  donc
- $$\zeta^{(k)}(x) \xrightarrow{x \rightarrow 0^+} 0.$$

Donc  $\zeta \in \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ .

□

## 15 Semaine 15

### 15.1 Inégalité de Jensen

Soit  $f : I \rightarrow \mathbb{R}$  convexe sur  $I$ .

Soit  $n \in \mathbb{N}^*$ . Soient  $x \in I^n$ ,  $\lambda \in [0; 1]^n$  telle que  $\sum_{k=1}^n \lambda_k = 1$ .

$$\sum_{k=1}^n \lambda_k x_k \in I \wedge f\left(\sum_{k=1}^n \lambda_k x_k\right) \leq \sum_{k=1}^n \lambda_k f(x_k) \quad (17)$$

*Démonstration.* Considérons le prédicat  $\mathcal{P}(\cdot)$  défini pour tout  $n \in \mathbb{N}^*$  par :

$$\mathcal{P}(n) : \text{“}\forall x \in I^n, \forall \lambda \in [0; 1]^n, \sum_{k=1}^n \lambda_k = 1 \implies \sum_{k=1}^n \lambda_k x_k \in I \wedge f\left(\sum_{k=1}^n \lambda_k x_k\right) \leq \sum_{k=1}^n \lambda_k f(x_k)\text{”}$$

\* Soient  $x \in I^1$  et  $\lambda \in [0; 1]^1$  tel que  $\sum_{k=1}^1 \lambda_k = 1$ .

Alors  $\lambda_1 = 1$ . Trivialement,  $\sum_{k=1}^1 \lambda_k x_k = \lambda_1 x_1 = x_1 \in I$ .

De plus,  $f\left(\sum_{k=1}^1 \lambda_k x_k\right) = f(\lambda_1 x_1) = f(x_1) = \lambda_1 f(x_1) = \sum_{k=1}^1 \lambda_k f(x_k)$ .

Donc  $\mathcal{P}(1)$  vrai.

\* Soit  $n \in \mathbb{N}^*$  tel que  $\mathcal{P}(n)$  vrai.

Soient  $x \in I^{n+1}$  et  $\lambda \in [0; 1]^{n+1}$  tel que  $\sum_{k=1}^{n+1} \lambda_k = 1$ .

$\{x_k \mid k \in \llbracket 1; n+1 \rrbracket\}$  est une partie non vide ( $n \geq 1$ ) d'un ensemble totalement ordonné  $(\mathbb{R}, \leq)$ .

Posons  $a = \min\{x_k \mid k \in \llbracket 1; n+1 \rrbracket\}$  et  $b = \max\{x_k \mid k \in \llbracket 1; n+1 \rrbracket\}$ . D'où

$$\underbrace{a}_{\sum_{k=1}^{n+1} \lambda_k = 1} \underset{\sum_{k=1}^{n+1} \lambda_k a \leq \sum_{k=1}^{n+1} \lambda_k x_k}{=} \sum_{k=1}^{n+1} \lambda_k a \underset{a \leq x_k}{\leq} \sum_{k=1}^{n+1} \lambda_k x_k \underset{x_k \leq b}{\leq} \sum_{k=1}^{n+1} \lambda_k b \underset{\sum_{k=1}^{n+1} \lambda_k = 1}{=} b$$

Or  $\{x_k \mid k \in \llbracket 1; n \rrbracket\} \subset I$  (car  $x \in I^n$ ) donc  $a \in I \wedge b \in I$ . Donc

$$\sum_{k=1}^{n+1} \lambda_k x_k \in [a; b] \underset{\substack{\subset \\ \text{par convexité} \\ \text{de l'intervalle } I}}{=} I$$

$\sum_{k=1}^{n+1} \lambda_k = 1$  donc  $\exists i_0 \in \llbracket 1; n+1 \rrbracket : \lambda_{i_0} \neq 1$  (sinon  $\sum_{k=1}^{n+1} \lambda_k = n+1 \neq 1$  car  $n \neq 0$ ).  
Fixons un tel  $i_0$ .

$$\begin{aligned} f\left(\sum_{k=1}^{n+1} \lambda_k x_k\right) &= f\left(\sum_{\substack{k=1 \\ k \neq i_0}}^{n+1} \lambda_k x_k + \lambda_{i_0} x_{i_0}\right) \\ &= f\left(\lambda_{i_0} x_{i_0} + (1 - \lambda_{i_0}) \sum_{\substack{k=1 \\ k \neq i_0}}^{n+1} \frac{\lambda_k}{1 - \lambda_{i_0}} x_k\right) \\ &\underset{\substack{\leq \\ \text{Par convexité} \\ \text{de } f}}{\leq} \lambda_{i_0} f(x_{i_0}) + (1 - \lambda_{i_0}) f\left(\sum_{\substack{k=1 \\ k \neq i_0}}^{n+1} \frac{\lambda_k}{1 - \lambda_{i_0}} x_k\right) \end{aligned}$$

Or  $\forall i \in \llbracket 1; n+1 \rrbracket \lambda_i \leq \sum_{\substack{k=1 \\ k \neq i_0}}^{n+1} \lambda_k = 1 - \lambda_{i_0}$  Donc  $\frac{\lambda_i}{1 - \lambda_{i_0}} \in [0; 1]$  et  $\sum_{\substack{k=1 \\ k \neq i_0}}^{n+1} \frac{\lambda_k}{1 - \lambda_{i_0}} = 1$ . Nous pouvons appliquer  $\mathcal{P}(n)$  pour  $\lambda_i \rightarrow \frac{\lambda_i}{1 - \lambda_{i_0}}$  :

$$\begin{aligned} f\left(\sum_{k=1}^{n+1} \lambda_k x_k\right) &\leq \lambda_{i_0} f(x_{i_0}) + (1 - \lambda_{i_0}) \sum_{\substack{k=1 \\ k \neq i_0}}^{n+1} \frac{\lambda_k}{1 - \lambda_{i_0}} f(x_k) \\ &\leq \lambda_{i_0} f(x_{i_0}) + \sum_{\substack{k=1 \\ k \neq i_0}}^{n+1} \lambda_k f(x_k) \\ &\leq \sum_{k=1}^{n+1} \lambda_k f(x_k) \end{aligned}$$

Donc  $\mathcal{P}(n+1)$  vrai. □

## 15.2 Inégalité arithmético-géométrique

Soit  $n \in \mathbb{N}^*$ . Soit  $x \in \mathbb{R}_+^{*n}$ .

$$\left(\prod_{k=1}^n x_k\right)^{1/n} \leq \frac{1}{n} \sum_{k=1}^n x_k \quad (18)$$

*Démonstration.* Soit de tels objets. Posons  $\forall k \in \llbracket 1; n \rrbracket, \lambda_k = 1/n$ .

Sachant que l'exponentielle est convexe, appliquons l'inégalité de Jensen pour  $x_k \leftarrow \ln(x_k)$  (autorisé car  $x_k \in \mathbb{R}_+^*$ ) :

$$\exp\left(\sum_{k=1}^n \frac{1}{n} \ln(x_k)\right) \leq \sum_{k=1}^n \frac{1}{n} \exp(\ln(x_k))$$

L'exponentielle est la bijection réciproque du logarithme népérien et est un morphisme additif. Nous obtenons ainsi l'inégalité recherchée. □



## 16 Semaine 16

### 16.1 Unicité de la partie régulière d'un développement limité

*Démonstration.* Soit  $f$  une fonction admettant un  $DL_n(x_0)$  avec  $n \in \mathbb{N}$  et  $x_0 \in \mathcal{D}_f$ . Supposons que  $f$  admette deux développements limités. C'est-à-dire qu'il existe  $a \in \mathbb{C}^{n+1}$  et  $b \in \mathbb{C}^{n+1}$  tels que :

$$f(x) \underset{x \rightarrow x_0}{=} \sum_{k=0}^n a_k (x - x_0)^k + o((x - x_0)^n)$$

$$f(x) \underset{x \rightarrow x_0}{=} \sum_{k=0}^n b_k (x - x_0)^k + o((x - x_0)^n)$$

Posons  $u = x - x_0$  et  $\tilde{f}(u) = f(x_0 + u)$  de sorte que les hypothèses sur  $f$  se traduisent par l'existence d'un  $DL_n(0)$  pour  $\tilde{f}$  :

$$f(x) \underset{x \rightarrow x_0}{=} \sum_{k=0}^n a_k u^k + o(u^n) \text{ et } f(x) \underset{x \rightarrow x_0}{=} \sum_{k=0}^n b_k u^k + o(u^n)$$

Appliquons la définition d'un  $DL_n(0)$ . Il existe deux fonctions  $\varepsilon_1$  et  $\varepsilon_2$  définies sur  $\mathcal{D}_{\tilde{f}}$  tels que

$$\forall u \in \mathcal{D}_{\tilde{f}}, \tilde{f}(u) = \sum_{k=0}^n a_k u^k + u^n \varepsilon_1$$

$$\forall u \in \mathcal{D}_{\tilde{f}}, \tilde{f}(u) = \sum_{k=0}^n b_k u^k + u^n \varepsilon_2$$

$$\lim_{u \rightarrow 0} \varepsilon_1(u) = 0 \text{ et } \lim_{u \rightarrow 0} \varepsilon_2(u) = 0$$

Donc

$$\forall u \in \mathcal{D}_{\tilde{f}}, \sum_{k=0}^n (a_k - b_k) u^k = u^n (\varepsilon_2(u) - \varepsilon_1(u))$$

Par l'absurde, supposons que  $\exists k_0 \in \llbracket 0; n \rrbracket : a_{k_0} \neq b_{k_0}$ . Posons  $k_1$  le plus petit entier dont les coefficients  $a$  et  $b$  sont différents :

$$k_1 = \min \{k \in \llbracket 0; n \rrbracket \mid a_k \neq b_k\}$$

Nous obtenons alors

$$\forall u \in \mathcal{D}_{\tilde{f}}, \sum_{k=0}^{k_1-1} \underbrace{(a_k - b_k)}_{=0} u^k + (a_{k_1} - b_{k_1}) u^{k_1} + \sum_{k=k_1+1}^n (a_k - b_k) u^k = u^n (\varepsilon_2(u) - \varepsilon_1(u))$$

Multiplions par  $u^{-k_1}$  puis calculons la limite en  $u \rightarrow 0$ . D'un côté, pour  $k > k_1$ , nous avons  $k - k_1 \leq 1$  donc  $(a_k - b_k) u^{k-k_1} \xrightarrow{u \rightarrow 0} 0$ . De l'autre côté,  $u^{n-k_1}$  tend vers 0 ou 1 selon si  $k_1 < n$  ou  $k_1 = n$ . Et, par hypothèse,  $\varepsilon_2(u) - \varepsilon_1(u) \xrightarrow{u \rightarrow 0} 0$ . Par unicité de la limite,  $a_{k_1} - b_{k_1} = 0$ . Ce qui contredit la définition de  $k_1$ .

Par conséquent  $\forall k \in \llbracket 0; n \rrbracket, a_k = b_k$ . Ainsi, la partie régulière d'un  $DL$  est unique.  $\square$

### 16.6 Deux fonctions équivalentes au voisinage de $a$ ont le même signe sur un voisinage de $a$

*Démonstration.* Soient  $f : \mathcal{D} \rightarrow \mathbb{R}$  et  $g : \mathcal{D} \rightarrow \mathbb{R}$  telles que  $f(x) \underset{x \rightarrow a}{\sim} g(x)$  avec  $a \in \mathcal{D}$ .

Appliquons la définition de l'équivalence pour  $\varepsilon \leftarrow \frac{1}{2}$ , il existe un voisinage  $V$  de  $a$  tel que :

$$\forall x \in V \cap \mathcal{D}, |f(x) - g(x)| \leq \frac{1}{2} |g(x)|$$

Fixons un tel voisinage  $V$ . Nous obtenons :

$$\forall x \in V \cap \mathcal{D}, \underbrace{g(x) - \frac{1}{2}|g(x)|}_{\text{du signe de } g(x)} \leq f(x) \leq \underbrace{g(x) + \frac{1}{2}|g(x)|}_{\text{du signe de } g(x)}$$

Ainsi  $f(x)$  et  $g(x)$  ont le même signe sur  $V \cap \mathcal{D}$ .  $\square$

## 16.7 Condition nécessaire et suffisante pour qu'une fonction $\mathcal{C}^\infty$ admette un extremum local ou un point d'inflexion

Soient  $f \in \mathcal{C}^\infty(\mathcal{D}, \mathbb{R})$  et  $a \in \overset{\circ}{\mathcal{D}}$ . Supposons que  $E_0 = \{p \in \mathbb{N}^* \setminus \{1\} \mid f^{(p)}(a) \neq 0\}$  est non vide. Posons  $p_0 = \min E_0$ .

$f$  admet un extremum local en  $a$  si et seulement si  $f'(a) = 0$  et  $p_0$  est pair.

$f$  admet un point d'inflexion en  $a$  si et seulement si  $p_0$  est impair.

*Démonstration.* Soient de tels objets. Traitons le cas de l'extremum local.  $f \in \mathcal{C}^\infty$  donc, la formule Taylor-Young donne un  $DL_{p_0}(a)$  de  $f$  :

$$f(x) \underset{x \rightarrow a}{=} \sum_{k=0}^{p_0} \frac{f^{(k)}(a)}{k!} (x-a)^k + o((x-a)^{p_0})$$

En développant :

$$f(x) \underset{x \rightarrow a}{=} f(a) + \underbrace{f'(a)(x-a)}_{=0} + \underbrace{\dots + \frac{f^{(p_0-1)}(a)}{(p_0-1)!} (x-a)^{p_0-1}}_{=0 \text{ par définition de } p_0} + \frac{f^{(p_0)}(a)}{p_0!} (x-a)^{p_0} + o((x-a)^{p_0})$$

Ainsi (car  $f^{(p_0)}(a) \neq 0$ )

$$f(x) - f(a) \underset{x \rightarrow a}{\sim} \frac{f^{(p_0)}(a)}{p_0!} (x-a)^{p_0} \quad (19)$$

Au voisinage de  $a$ ,  $f(x) - f(a)$  et  $\frac{f^{(p_0)}(a)}{p_0!} (x-a)^{p_0}$  ont le même signe.

Supposons que  $f$  admette un extremum local en  $a$ . Or  $a \in \overset{\circ}{\mathcal{D}}$  et  $f$  est dérivable en 0, donc  $f'(a) = 0$ . Comme  $f$  admette un extremum local en  $a$ ,  $f(x) - f(a)$  est de signe constant au voisinage de  $a$ . Donc  $\frac{f^{(p_0)}(a)}{p_0!} (x-a)^{p_0}$  est de signe constant au voisinage de  $a$ . Par conséquent,  $p_0$  est pair.

Réciproquement, supposons que  $f'(a) = 0$  et que  $p_0$  est pair.  $\frac{f^{(p_0)}(a)}{p_0!} (x-a)^{p_0}$  est de signe constant au voisinage de  $a$ . Donc  $f(x) - f(a)$  est de signe constant au voisinage de  $a$ . Ainsi,  $a$  est un extremum local de  $f$ .

Traitons le cas du point d'inflexion. La formule de Taylor-Young donne :

$$f(x) - \underbrace{(f(a) + (x-a)f'(a))}_{\text{tangente en } (a, f(a))} \underset{x \rightarrow a}{\sim} \frac{f^{(p_0)}(a)}{p_0!} (x-a)^{p_0} \quad (20)$$

Le signe de l'écart courbe/tangente en  $a$  est donc celui de  $\frac{f^{(p_0)}(a)}{p_0!} (x-a)^{p_0}$ . Ce qui conclut de la même manière que l'extremum local.  $\square$

## 17 Semaine 17

### 17.4 Théorème de Bézout

Soient  $a, b \in \mathbb{N}^*$  et  $c \in \mathbb{Z}$ . Il existe des entiers  $x, y \in \mathbb{Z}$  tels que  $ax + yb = c$  si et seulement si  $c$  est multiple du pgcd de  $a$  et  $b$ .

*Démonstration.* Soient  $a, b \in \mathbb{N}^*$ . On suppose l'algorithme d'Euclide réalisé pour  $a, b$ , ainsi à la fin de ce dernier on a un entier naturel  $r_n$  tel que  $r_n = a \wedge b$ . Comme l'algorithme est terminé, on peut remonter chaque ligne de proche en proche, on aurait, à titre d'exemple, pour une première itération,  $r_n = r_{n-2} - q_n \cdot r_{n-1}$ . En réalisant toutes les étapes nécessaires, on obtient une relation entre  $r_n$  et  $a, b$ , cette relation s'écrit :

$$\exists (x_0, y_0) \in (\mathbb{Z}^*)^2 : a \wedge b = r_n = ax_0 + y_0b.$$

Si  $c$  est un multiple de  $a \wedge b$ , alors il existe  $k \in \mathbb{Z}^*$  tel que  $c = k(a \wedge b)$ , donc en multipliant le résultat montré au dessus par  $k$ , on a le sens indirect. Si pour  $c \in \mathbb{Z}$ , il existe des entiers  $x, y \in \mathbb{Z}$  tels que  $ax + yb = c$ , alors le pgcd de  $a$  et  $b$  divise le membre de gauche et donc par égalité le membre de droite aussi donc  $c$  est multiple de  $a \wedge b$ , ce qui suffit.  $\square$

### 17.6 Théorème de Gauss

Soient  $a, b, c$  trois entiers naturels non nuls. Si  $c$  est premier avec  $a$  et divise le produit  $ab$ , alors il divise  $b$ .

*Démonstration.* Soient  $a, b, c$  des entiers naturels vérifiant les hypothèses.

Comme  $c$  est premier avec  $a$  on écrit une relation de Bézout pour 1, leur pgcd et on multiplie le tout par  $b$  :

$$\exists (u, v) \in (\mathbb{N}^*)^2 : au + vc = 1 \implies abu + vbc = b,$$

or  $c$  divise  $ab$  et lui-même donc aussi le membre de gauche donc par égalité, le membre droite, c'est le théorème.  $\square$

### 17.8 Résoudre une équation du type $ax + yb = c$

Soient  $a, b, c \in \mathbb{Z}$ . Résoudre l'équation

$$ax + yb = c,$$

d'inconnues  $x$  et  $y$  dans  $\mathbb{Z}$ .

*Démonstration.* Soient  $a, b, c \in \mathbb{Z}$  et une telle équation, notée (i), en lesdites inconnues.

Si  $a \wedge b \nmid c$ , alors le théorème de Bézout, affirme que l'équation n'a pas de solution.

Supposons le contraire. Posons  $d = a \wedge b$ . Le lemme technique affirme l'existence de  $a'$  et  $b'$  dans  $\mathbb{Z}$ , tels que  $a'd = a$ ,  $b'd = b$  et  $a' \wedge b' = 1$ . Donc, comme  $d$  divise  $c$ , il existe  $c'$  tel que  $c = c'd$ . On réécrit l'équation, notée (ii) :

$$a'x + yb' = c'.$$

On sait d'après le théorème de Bézout qu'il existe des solutions, en particulier grâce à l'algorithme d'Euclide on construit  $(x_0, y_0)$ , une solution de la nouvelle équation, puis on l'injecte et on raisonne par équivalence, on note  $\omega$  l'ensemble des solutions de (ii) et  $\Omega$  celui de (i) :

$$\begin{aligned} (x, y) \in \Omega &\iff (x, y) \in \omega \\ &\iff a'x + yb' = c' \\ &\iff a'x + yb' = a'x_0 + y_0b' \\ &\iff a'(x - x_0) = b'(y_0 - y) \\ &\iff \exists k \in \mathbb{Z} : \begin{cases} a'(x - x_0) &= b'(y_0 - y) \\ y_0 - y &= a'k \end{cases} \\ &\iff \exists k \in \mathbb{Z} : \begin{cases} a'(x - x_0) &= b'(y_0 - y) \\ y &= y_0 - a'k \end{cases} \\ &\iff \exists k \in \mathbb{Z} : \begin{cases} x &= x_0 + b'k \\ y &= y_0 - a'k \end{cases} \\ &\iff (x, y) \in \{(x_0 + b'k, y_0 - a'k) \mid k \in \mathbb{Z}\} \end{aligned}$$

La première ligne découle de la divisibilité des coefficients par  $d$ , la deuxième est la définition d'appartenance à  $\omega$ , la troisième est une réécriture du fait que  $(x_0, y_0)$  soit solution de (ii), la quatrième est une factorisation banale, la cinquième une utilisation du théorème de Gauss pour le sens direct et le sens indirect ne pose pas de problème, la sixième est une réécriture de la deuxième relation, la septième découle de l'expression de  $y$  pour le sens direct et le sens indirect s'obtient en multipliant avec parcimonie l'équation, la huitième est une réécriture de la septième qui ne pose pas de problème. C'est  $\Omega$ , par équivalence.

□

## 18 Semaine 18

### 18.1 L'ensemble des nombres premiers est infini

*Démonstration.* Notons l'ensemble des nombres premiers  $\mathcal{P} = \{n \in \mathbb{N} \mid |\mathcal{D}(n) \cup \mathbb{N}| = 2\}$ . Par l'absurde, supposons que  $\mathcal{P}$  est fini.

Posons  $m = 1 + \prod_{p \in \mathcal{P}} p \in \mathbb{N}$ .

Comme  $2 \in \mathcal{P}$ ,  $m \geq 2$ . Donc  $m$  admet un diviseur premier,  $\exists q \in \mathcal{P} : q \mid m$ . Donc  $q \wedge m = q$ .

Par ailleurs,  $m = 1 + q \left( \prod_{\substack{p \in \mathcal{P} \\ p \neq q}} p \right)$ . Donc  $m - q \left( \prod_{\substack{p \in \mathcal{P} \\ p \neq q}} p \right) = 1$ . D'après le théorème de Bézout,

$q \wedge m = 1$ .

Donc  $q = 1$  ce qui est une contradiction avec  $q \in \mathcal{P}$ .  $\square$

### 18.2 Caractérisation de la valuation $p$ -adique

Soit  $n \in \mathbb{N}^*$ ,  $p \in \mathcal{P}$ ,  $k_0 \in \mathbb{N}$ .

$$\nu_p(n) = k_0 \iff \exists m \in \mathbb{Z} : \begin{cases} n = p^{k_0} m \\ m \wedge p = 1 \end{cases} \quad (21)$$

*Démonstration.*  $\implies$  Supposons que  $\nu_p(n) = k_0$ .

Par définition de la valuation  $p$ -adique,  $p^{\nu_p(n)} \mid n$  donc  $p^{k_0} \mid n$ . Notons  $m \in \mathbb{Z}$  le quotient de la division euclidienne de  $n$  par  $p^{k_0}$ . Nous avons  $n = p^{k_0} m$ .

Comme  $m \wedge p \in \mathcal{D}(p) \cap \mathbb{N}$ ,  $m \wedge p \in \{1, p\}$ . Par l'absurde, supposons que  $m \wedge p = p$ .

$$\begin{aligned} p \mid m &\implies \exists m' \in \mathbb{Z} : m = pm' \\ &\implies \exists m' \in \mathbb{Z} : n = pp^{k_0} m' = p^{k_0+1} m' \\ &\implies k_0 + 1 \in \{k \in \mathbb{N} \mid p^k \mid n\} \\ &\implies k_0 + 1 \leq \max \{k \in \mathbb{N} \mid p^k \mid n\} = \nu_p(n) = k_0 \end{aligned}$$

Ce qui est une contradiction donc  $m \wedge p = 1$ .

$$\Leftarrow \text{Supposons } \exists m \in \mathbb{Z} : \begin{cases} n = p^{k_0} m \\ m \wedge p = 1 \end{cases}$$

Par définition de la valuation  $p$ -adique,  $p^{\nu_p(n)} \mid n$  donc  $p^{\nu_p(n)} \mid p^{k_0} m$ . Or  $m \wedge p = 1$  donc  $m \wedge p^{\nu_p(n)} = 1$ . D'après le théorème de Gauss,  $p_{\nu_p(n)} \mid p^{k_0}$ . Donc  $\exists \alpha \in \mathbb{Z} : \alpha p_{\nu_p(n)} = p^{k_0}$

$$\begin{aligned} \alpha p_{\nu_p(n)} = p^{k_0} &\implies p^{k_0} - \alpha p_{\nu_p(n)} = 0 \\ &\implies p^{k_0} (1 - \alpha p^{\nu_p(n) - k_0}) = 0 \text{ car } k_0 \leq \nu_p(n) \\ &\implies \alpha p^{\nu_p(n) - k_0} = 1 \text{ car } \mathbb{Z} \text{ est int\`egre} \\ &\implies p^{\nu_p(n) - k_0} \in \mathcal{D}(1) \cap \mathbb{N} \\ &\implies p^{\nu_p(n) - k_0} = 1 \\ &\implies \nu_p(n) - k_0 = 0 \\ &\implies \nu_p(n) = k_0 \end{aligned}$$

$\square$

### 18.3 Caractérisation de $a \mid b$ par les valuations $p$ -adiques et preuve de leur propriété de morphisme.

$$\forall (a, b) \in \mathbb{Z}^2, a \mid b \iff \forall p \in \mathcal{P}, \nu_p(a) \leq \nu_p(b) \quad (22)$$

*Démonstration.* Premièrement, montrons que la valuation  $p$ -adique est un morphisme de  $(\mathbb{Z}^*, \times)$  dans  $(\mathbb{N}, +)$ .

Soient de tels entiers relatifs  $a, b$ .

$$\exists m, n \in (\mathbb{Z}^*)^2 : \left( (a = p^{\nu_p(a)} m) \wedge (m \wedge p = 1) \right) \wedge \left( (b = p^{\nu_p(b)} n) \wedge (n \wedge p = 1) \right),$$

donc  $ab = p^{\nu_p(a) + \nu_p(b)} mn$  et  $mn \wedge p = 1$ , par la réciproque de la caractérisation des valuations  $p$ -adiques :

$$\nu_p(ab) = \nu_p(a) + \nu_p(b).$$

Prouvons le sens réciproque de la susdite caractérisation. Supposons le membre de droite.

D'après le théorème de décomposition en facteurs premiers,

$$|b| = \prod_{p \in \mathcal{P}} p^{\nu_p(b)} = \prod_{p \in \mathcal{P}} p^{\nu_p(a)} (p^{\nu_p(b) - \nu_p(a)}) = \prod_{p \in \mathcal{P}} p^{\nu_p(a)} \prod_{p \in \mathcal{P}} p^{\nu_p(b) - \nu_p(a)} = |a| \prod_{p \in \mathcal{P}} p^{\nu_p(b) - \nu_p(a)},$$

la première manipulation se justifie par hypothèse et la seconde peut se justifier par le calcul.

Ainsi,  $|a| \mid |b|$  donc  $a \mid b$ .

Prouvons le sens direct. Supposons le membre de gauche.

Soit  $p \in \mathcal{P}$ . Il existe  $k \in \mathbb{Z}$  tel que  $ak = b$  car  $a \mid b$ . Ainsi,

$$\nu_p(b) = \nu_p(ak) = \nu_p(a) + \nu_p(k) \geq \nu_p(a).$$

Ce qui suffit. □

## 18.4 Expression du pgcd et du ppcm à partir des décomposition en facteurs premiers de $a$ et $b$ .

Le pgcd comme produit des  $p$  à la puissance du minimum des  $\nu_p$  et le ppcm comme le produit des  $p$  à la puissance du maximum des  $\nu_p$ .

$$\begin{aligned} a \wedge b &= \prod_{p \in \mathcal{P}} p^{\min(\nu_p(a), \nu_p(b))} \\ a \vee b &= \prod_{p \in \mathcal{P}} p^{\max(\nu_p(a), \nu_p(b))} \end{aligned} \tag{23}$$

*Démonstration.* Prouvons la formule du pgcd et déduisons-en la formule du ppcm.

Soient  $(a, b) \in (\mathbb{Z}^*)^2$ . Soit  $p \in \mathcal{P}$ . Il faut et il suffit de montrer que  $\nu_p(a \wedge b) = \min(\nu_p(a), \nu_p(b))$  pour obtenir le résultat. On a  $a \wedge b \mid a$  et  $a \wedge b \mid b$  donc d'après la caractérisation de la divisibilité par les valuations  $p$ -adiques,  $\nu_p(a \wedge b) \leq \nu_p(a)$  et  $\nu_p(a \wedge b) \leq \nu_p(b)$  donc  $\nu_p(a \wedge b) \leq \min(\nu_p(a), \nu_p(b))$ . Posons  $m = \min(\nu_p(a), \nu_p(b))$ . On a

$$|a| = \prod_{q \in \mathcal{P}} q^{\nu_q(a)} = p^m \left( (p^{\nu_p(a) - m}) \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(a)} \right),$$

car par définition,  $m \leq \nu_p(a)$ , donc  $p^m \mid a$ , on montrerait de même que  $p^m \mid b$ , donc par définition,  $p^m \mid a \wedge b$ , donc une nouvelle fois en appliquant la caractérisation de la divisibilité par les valuations  $p$ -adiques,  $m \leq \nu_p(a \wedge b)$ . Finalement,  $\nu_p(a \wedge b) = m$ .

On en déduit la formule du ppcm :

$$|a||b| = (a \wedge b)(a \vee b) \implies a \vee b = \prod_{p \in \mathcal{P}} p^{\nu_p(a) + \nu_p(b) - \min(\nu_p(a), \nu_p(b))} = \prod_{p \in \mathcal{P}} p^{\max(\nu_p(a), \nu_p(b))}$$

□

## 18.5 Pour $p$ premier, $(a + b)^p \equiv a^p + b^p \pmod{p}$ , en déduire le petit Th. de Fermat (2 versions), expression du résultat dans $\mathbb{Z}/p\mathbb{Z}$ .

Petit Th. de Fermat :

- (i)  $\forall a \in \mathbb{Z}, a^p \equiv a \pmod{p}$   
 $\forall x \in \mathbb{Z}/p\mathbb{Z}, x^p = x$
- (ii)  $\forall a \in \mathbb{Z}, p \nmid a, \implies a^{p-1} \equiv 1 \pmod{p}$   
 $\forall x \in \mathbb{Z}/p\mathbb{Z}, x^{p-1} = 1$

*Démonstration.* Soient  $a, b$  de tels entiers relatifs et soit  $p$  un nombre premier. Calculons,

$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k \equiv a^p + b^p \pmod{p},$$

car  $\forall k \in \llbracket 1, p-1 \rrbracket$ ,  $p \mid \binom{p}{k}$  (élémentaire), d'où le résultat.

Dans  $\mathbb{Z}/p\mathbb{Z}$ , ce résultat s'énonce comme suit :

$$\forall (x, y) \in \mathbb{Z}/p\mathbb{Z}^2, (x+y)^p = x^p + y^p.$$

En guise d'application, démontrons le petit Th. de Fermat énoncé plus haut.

Démonstration du (i). Considérons le prédicat  $\mathcal{P}(\cdot)$  défini sur  $\mathbb{N}$  par :

$$\mathcal{P}(a) : "a^p \equiv a \pmod{p}."$$

Initialisation : Pour  $a = 0$ , rien à faire, donc  $\mathcal{P}(0)$  est vrai.

Hérédité : Soit  $a \in \mathbb{N}$  tel que  $\mathcal{P}(a)$ . Calculons,

$$(a+1)^p \equiv a^p + 1 \pmod{p} \stackrel{\mathcal{P}(a)}{\equiv} a + 1 \pmod{p},$$

donc  $\mathcal{P}(a+1)$  vrai.

Par Th. de récurrence sur  $\mathbb{N}$ ,  $\mathcal{P}(a)$  est vrai pour tout  $a \in \mathbb{N}$ .

Il faut maintenant étendre le résultat à  $\mathbb{Z}$ . Soit  $p \in \mathcal{P} \setminus \{2\}$ , ainsi  $p$  est impair. Soit  $a \in \mathbb{Z} \setminus \mathbb{N}$ .

Calculons,

$$a^p \equiv (-|a|)^p \pmod{p} \equiv -|a|^p \pmod{p} \stackrel{\text{Th. de Fermat pour } a \leftarrow |a|}{\equiv} -|a| \pmod{p} \equiv a \pmod{p}.$$

Si  $p = 2$ ,  $a^2 \equiv |a|^2 \pmod{2} \equiv |a| \pmod{2} \equiv -|a| \pmod{2} \equiv a \pmod{2}$ .

Le (ii), soit  $a \in \mathbb{Z}$  tel que  $p \nmid a$ .

$$(p \nmid a) \wedge (p \in \mathcal{P}) \implies p \wedge a = 1,$$

d'après le (i),  $p \mid a^p - a \implies p \mid a(a^{p-1} - 1) \stackrel{\text{Th. de Gauss}}{\implies} p \mid a^{p-1} - 1 \implies a^{p-1} \equiv 1 \pmod{p}$ .

Les écritures dans  $\mathbb{Z}/p\mathbb{Z}$  ne posent pas de problème.s, ce qui conclut.  $\square$

## 18.6 $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n$ est premier.

*Démonstration.* Montrons le sens réciproque, supposons  $n \in \mathcal{P}$ .

Soit  $x \in \mathbb{Z}/n\mathbb{Z}$  tel que  $x \neq \bar{0}$ .

$\exists a \in \llbracket 0, p-1 \rrbracket : c = \bar{a}$ ,  $I = \llbracket 0, p-1 \rrbracket$  étant un système de représentant des classes.

Comme  $a \in I$ ,  $n \nmid a$ , or  $n \in \mathcal{P}$ , donc  $n \wedge a = 1$ . Par Bezout, il existe  $u, v \in \mathbb{Z}^2$  tels que  $au + nv = 1$ , donc  $u$  est l'inverse de  $a$  modulo  $n$  donc  $a \in \mathbb{Z}/n\mathbb{Z}^\times$ , dès lors, tout élément non nul de  $\mathbb{Z}/n\mathbb{Z}$  est inversible, or c'est un anneau commutatif, donc c'est un corps.

Montrons le sens direct en raisonnant par contraposition, supposons  $n \notin \mathcal{P}$ .

Comme  $n$  n'est pas premier et est plus grand que 2, il admet un diviseur,  $d$ , dans  $I \setminus \{0, 1\} = J$ . Notons  $d'$  le quotient de la division euclidienne de  $n$  par  $d$ , on a alors  $n = dd'$  et  $d' \in J$ . Donc  $\bar{d}\bar{d}' = \bar{0}$  et comme  $d, d' \in J$ , on a  $d, d' \neq 0$ , donc  $\bar{d}$  est un diviseur de zéro de  $\mathbb{Z}/n\mathbb{Z}$ , donc  $\bar{d}$  est un élément non nul de  $\mathbb{Z}/n\mathbb{Z}$  non inversible, donc  $\mathbb{Z}/n\mathbb{Z}$  n'est pas un corps. En contraposant ce que nous venons de démontrer on a le résultat. Ce qui conclut.  $\square$

## 18.7 Les éléments inversibles d'un anneau $A$ forment un groupe multiplicatif noté $(A^\times, \times)$

*Démonstration.* Soit  $(A, +, \times)$  un anneau.

Un élément inversible (ou unité) est un élément de  $A$  symétrisable pour la loi  $\times$ . Posons l'ensemble des éléments inversibles  $A^\times = \{a \in A \mid \exists b \in A : a \times b = b \times a = 1_A\}$ .

★ Montrons que la LCI  $\times$  se restreint bien à  $A^\times$  en un LCI  $\times_{A^\times}$ .

Soient  $(a_1, a_2) \in A^{\times 2}$ . Par définition de  $A^\times$ ,  $\exists (b_1, b_2) \in A^2 : a_1 \times b_1 = b_1 \times a_1 = 1_A$  et  $a_2 \times b_2 = b_2 \times a_2 = 1_A$ .

$$(a_1 \times a_2) \times (b_2 \times b_1) \stackrel{\text{loi associative}}{=} a_1 \times \underbrace{a_2 \times b_2}_{= 1_A} \times b_1 = a_1 \times b_1 = 1_A$$

$$(b_2 \times b_1) \times (a_1 \times a_2) \underset{\text{loi associative}}{=} b_2 \times \underbrace{b_1 \times a_1}_{= 1_A} \times a_2 = b_2 \times a_2 = 1_A$$

Donc  $(a_1 \times a_2) \in A^\times$ .

- ★ La loi  $\times$  est associative donc la loi  $\times_{A^\times}$  l'est aussi.
- ★  $1_A$  vérifie  $1_A \times 1_A = 1_A$  donc  $1_A \in A^\times$ .  
De plus,  $\forall a \in A^\times, 1_A \times_{A^\times} a = a \times_{A^\times} 1_A = a$  donc  $\times_{A^\times}$  admet  $1_A$  comme élément neutre.
- ★ Soit  $a \in A^\times$ . Par définition de  $A^\times$ ,  $\exists b \in A : a \times b = b \times a = 1_A$ .  
D'où  $b \in A^\times$ . En pensant les égalités ci-dessus dans  $A^\times$ ,

$$a \times_{A^\times} b = b \times_{A^\times} a = 1_A$$

Donc  $a$  est inversible dans  $A^\times$ .

Ainsi,  $(A^\times, \times_{A^\times})$  est un groupe. □

## 18.8 L'image directe par un morphisme d'anneau d'un sous-anneau de l'anneau de départ est un sous anneau de l'anneau d'arrivée. De même pour l'image réciproque.

*Démonstration.* Soient  $(A, +, \times)$  et  $(B, +, \times)$  deux anneaux et  $f : A \rightarrow B$  un morphisme d'anneau. Soit  $A'$  un sous-anneau de  $A$ . Montrons que  $f(A')$  est un sous-anneau de  $B$ .

- ★ Par définition de  $f$ ,  $f(A') \subset B$  et  $(B, +, \times)$  est un anneau.
- ★ Soient  $(u, v) \in f(A')^2$ . Alors  $\exists (a, b) \in A'^2 : f(a) = u$  et  $f(b) = v$ .  $f$  est un morphisme d'anneau donc un morphisme de groupe de  $(A, +)$  dans  $(B, +)$  donc

$$u - v = f(a) - f(b) = f(a - b)$$

Comme  $A'$  est un sous-anneau,  $a - b \in A'$ . Donc  $u - v \in f(A')$ .

De même,  $f$  est un morphisme d'anneau donc un morphisme de monoïde de  $(A, \times)$  dans  $(B, \times)$  donc

$$u \times v = f(a) \times f(b) = f(a \times b)$$

Comme  $A'$  est un sous-anneau,  $a \times b \in A'$ . Donc  $u \times v \in f(A')$ .

- ★  $f$  est un morphisme d'anneau donc  $1_B = f(1_A)$ . Or  $A'$  est un sous-anneau donc  $1_A \in A'$ . D'où  $1_B \in f(A')$ .

Soit  $B'$  un sous-anneau de  $B$ . Montrons que  $f^{-1}(B')$  est un sous-anneau de  $A$ .

- ★ Par définition de  $f$ ,  $f^{-1}(B') \subset A$  et  $(A, +, \times)$  est un anneau.
- ★ Soient  $(a, b) \in f^{-1}(B')^2$ .  $f$  est un morphisme d'anneau donc un morphisme de groupe de  $(A, +)$  dans  $(B, +)$  donc

$$f(a - b) = \underbrace{f(a)}_{\in B'} - \underbrace{f(b)}_{\in B'} \in B'$$

Donc  $a - b \in f^{-1}(B')$ .

De même,  $f$  est un morphisme d'anneau donc un morphisme de monoïde de  $(A, \times)$  dans  $(B, \times)$  donc

$$f(ab) = \underbrace{f(a)}_{\in B'} \underbrace{f(b)}_{\in B'} \in B'$$

Donc  $ab \in f^{-1}(B')$ .

- ★  $f$  est un morphisme d'anneau donc  $1_B = f(1_A)$ . Or  $B'$  est un sous-anneau donc  $1_B \in B'$ . D'où  $1_A \in f^{-1}(B')$ .

□



## 19 Semaine 19

**19.1**  $(A \times B)^T = B^T \times A^T$

Pour une matrice  $A \in \mathcal{M}_{(n,p)}(\mathbb{K})$ , la matrice transposée est définie :

$$\forall (k, l) \in \llbracket 1, p \rrbracket \times \llbracket 1, n \rrbracket, [A^T]_{kl} = A_{lk}$$

Formellement, la transposition est une application de  $\mathcal{M}_{(n,p)}(\mathbb{K})$  dans  $\mathcal{M}_{(p,n)}(\mathbb{K})$ .

*Démonstration.* Soit  $(A, B) \in \mathcal{M}_{(n,p)}(\mathbb{K}) \times \mathcal{M}_{(p,q)}(\mathbb{K})$ .

$(A \times B)^T \in \mathcal{M}_{(q,n)}(\mathbb{K})$ . Soit  $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, n \rrbracket$ .

$$\begin{aligned} [(A \times B)^T]_{i,j} &= [A \times B]_{j,i} \\ &= \sum_{k=1}^p A_{j,k} \times_{\mathbb{K}} B_{k,i} \\ &= \sum_{k=1}^p B_{k,i} \times_{\mathbb{K}} A_{j,k} \\ &= \sum_{k=1}^p [B^T]_{i,k} \times_{\mathbb{K}} [A^T]_{k,j} \\ &= [(B^T) \times (A^T)]_{i,j} \end{aligned}$$

□

## 19.2 Calculer $E^{i,j} \times E^{k,l}$ en fonction de $i, j, k, l$ et des symboles de Kronecker

Le symbole de Kronecker est défini de la manière suivante :

$$\forall (x, y) \in \mathbb{R}^2, \delta_{xy} = \begin{cases} 0 & \text{si } x \neq y \\ 1 & \text{si } x = y \end{cases}$$

La matrice  $E^{i,j} \in \mathcal{M}_{(n,p)}(\mathbb{K})$  avec  $(i, j) \in \llbracket 1, n \rrbracket \times \llbracket 1, p \rrbracket$  ne possède que des coefficients nuls sauf le coefficient de la  $i^e$  ligne et  $j^e$  colonne qui vaut 1. Formellement :

$$\forall (r, s) \in \llbracket 1, n \rrbracket \times \llbracket 1, p \rrbracket, [E^{i,j}]_{rs} = \delta_{ir} \delta_{js}$$

*Démonstration.* Calculons  $E^{i,j}(n, p) \times E^{k,l}(p, q)$ .

Soient  $(r, s) \in \llbracket 1, n \rrbracket \times \llbracket 1, q \rrbracket$  fq

$$\begin{aligned} [E^{i,j} \times E^{k,l}]_{rs} &= \sum_{t=1}^p E_{r,t}^{i,j} E_{t,s}^{k,l} \\ &= \sum_{t=1}^p \delta_{ir} \delta_{jt} \delta_{kt} \delta_{ls} \\ &= \delta_{jk} \delta_{ir} \delta_{ls} \\ &= \delta_{jk} [E^{i,l}]_{rs} \end{aligned}$$

Donc  $E^{i,j} \times E^{k,l} = \delta_{jk} E^{i,l}$ .

Ainsi, pour le calcul de  $(E^{i,j})^2$ ,  $q \leftarrow n$ ,  $k \leftarrow i$ ,  $l \leftarrow j$ .

$$(E^{i,j})^2 = \delta_{ji} E^{i,j} = \begin{cases} E^{i,j} & \text{si } i = j \\ 0_{n,p} & \text{si } i \neq j \end{cases}$$

□

### 19.3 Les matrices triangulaires supérieures forment un sous-anneau de $\mathcal{M}_n(\mathbb{K})$

*Démonstration.*  $\mathcal{T}_n^+(\mathbb{K}) \subset (M)_n(\mathbb{K})$  et  $(\mathcal{M}_n(\mathbb{K}), +, \times)$  est un anneau.

$\mathcal{T}_n^+(\mathbb{K}) \neq \emptyset$  car  $I_n \in \mathcal{T}_n^+(\mathbb{K})$  ( $I_n$  est le neutre multiplicatif de  $\mathcal{M}_n(\mathbb{K})$ ).

Soient  $(A, B) \in \mathcal{T}_n^+(\mathbb{K})^2$ .

Soient  $(i, j) \in \llbracket 1, n \rrbracket^2$  tels que  $i > j$ .

$$(A - B)_{i,j} = \underbrace{A_{i,j}}_{=0 \text{ car } A \in \mathcal{T}_n^+(\mathbb{K})} - \underbrace{B_{i,j}}_{=0 \text{ car } B \in \mathcal{T}_n^+(\mathbb{K})} = 0$$

Donc,  $A - B \in \mathcal{T}_n^+(\mathbb{K})$ .

$$\begin{aligned} (A \times B)_{i,j} &= \sum_{k=1}^n A_{i,k} \times_{\mathbb{K}} B_{k,j} \\ &= \sum_{k=1}^j \underbrace{A_{i,k}}_{=0 \text{ car } i > j \geq k \text{ et } A \in \mathcal{T}_n^+(\mathbb{K})} \times_{\mathbb{K}} B_{k,j} + \sum_{k=j+1}^n A_{i,k} \times_{\mathbb{K}} \underbrace{B_{k,j}}_{=0 \text{ car } k > j \text{ et } B \in \mathcal{T}_n^+(\mathbb{K})} \\ &= 0 \end{aligned}$$

Donc,  $A \times B \in \mathcal{T}_n^+(\mathbb{K})$ . □

### 19.4 Si $A$ est une matrice d'ordre $n$ et $\lambda$ un scalaire non nul d'un corps, alors la transposée de $A$ et $\lambda A$ sont inversibles aussi.

*Démonstration.* Soient  $A, \lambda \in \mathcal{GL}_n(\mathbb{K}) \times \mathbb{K}^*$ , avec  $\mathbb{K}$  un corps.

Par définition, il existe  $B \in \mathcal{GL}_n(\mathbb{K})$  tel que  $AB = BA = I_n$ . Ainsi :

$$(AB)^T = I_n^T \iff B^T A^T = I_n,$$

donc  $A^T$  admet un inverse à gauche,  $B^T$ , donc un inverse tout court et donc  $A^T$  est inversible (on notera que  $A^T$  reste dans les matrices d'ordre  $n$ ). De même,

$$\lambda AB = \lambda I_n \iff (\lambda A)B = \lambda I_n \iff (\lambda A) \left( \frac{1}{\lambda} B \right) = I_n,$$

car les scalaires commutent avec toutes les matrices. Ainsi,  $\lambda A$  admet un inverse à droite, donc un inverse tout court, donc est inversible, d'inverse  $\frac{1}{\lambda} B$ . Concluant la preuve. □

### 19.5 Si $N$ est une matrice d'ordre $n$ nilpotente, alors $I_n + \lambda N$ est inversible pour tout $\lambda$ , scalaire d'un corps.

*Démonstration.* Soient  $N$  une matrice d'ordre  $n$  à coefficient dans  $\mathbb{K}$ , un corps, nilpotente, d'indice de nilpotence  $k$  (un entier naturel donc) et  $\lambda \in \mathbb{K}$ . Calculons :

$$I_n^{2k+1} + (\lambda N)^{2k+1} = I_n^{2k+1} - (-\lambda N)^{2k+1} = (I_n + \lambda N) \sum_{i=0}^{2k} (-\lambda N)^i = (I_n + \lambda N) \sum_{i=0}^{k-1} (-\lambda N)^i,$$

car  $\lambda N$  commute avec  $I_n$ , or le membre de gauche est égal à  $I_n$  car  $2k + 1 > k$ , donc  $I_n + \lambda N$  est inversible à droite, donc inversible tout court, d'inverse  $\sum_{i=0}^{k-1} (-\lambda N)^i$ . Ce qui conclut la preuve. □

### 19.6 Caractérisation de l'inversibilité pour les matrices

$A \in \mathcal{M}_n(\mathbb{K})$  est inversible si et seulement si pour tout  $Y \in \mathcal{M}_{n,1}(\mathbb{K})$ , l'équation  $AX = Y$  d'inconnue  $X \in \mathcal{M}_{n,1}$  admet une unique solution.

$$\forall A \in \mathcal{M}_n(\mathbb{K}), A \in \mathcal{GL}_n(\mathbb{K}) \iff \forall Y \in \mathcal{M}_{n,1}(\mathbb{K}), \exists! X \in \mathcal{M}_{n,1} : AX = Y \quad (24)$$

*Démonstration.* Supposons que  $A \in \mathcal{GL}_n(\mathbb{K})$ . Soit  $Y \in \mathcal{M}_{n,1}(\mathbb{K})$  fixé quelconque.  
 $AX = Y \iff A^{-1}AX = A^{-1}Y \iff X = A^{-1}Y$  donc l'équation  $AX = Y$  d'inconnue  $X \in \mathcal{M}_{n,1}$  admet une unique solution.

Supposons maintenant que  $\forall Y \in \mathcal{M}_{n,1}(\mathbb{K}), \exists! X \in \mathcal{M}_{n,1} : AX = Y$ .  
 Pour  $i \in \llbracket 1; n \rrbracket$ , notons  $X_i$  la solution de  $AX = E^{i,1}$ .

Posons  $B = \left[ \begin{array}{c|c|c|c} X_1 & X_2 & \dots & X_n \end{array} \right]$ .

Calculons  $AB = \left[ \begin{array}{c|c|c|c} AX_1 & AX_2 & \dots & AX_n \end{array} \right] = \left[ \begin{array}{c|c|c|c} E^{1,1} & E^{2,1} & \dots & E^{n,1} \end{array} \right] = I_n$ .

Ainsi A est inversible à droite donc  $A \in \mathcal{GL}_n(\mathbb{K})$  et  $A^{-1} = B$ . □

## 19.7 Caractérisation des matrices diagonales inversibles

Une matrice diagonale est inversible si et seulement si tous ses coefficients diagonaux sont non nuls.

$$\forall D = \text{diag}(d_1, d_2, \dots, d_n) \in \mathcal{D}_n(\mathbb{K}), D \in \mathcal{GL}_n(\mathbb{K}) \iff \prod_{i=1}^n d_i \neq 0 \quad (25)$$

*Démonstration.* Soit  $D \in \mathcal{D}_n(\mathbb{K})$  de coefficients diagonaux  $d_1, d_2, \dots, d_n \in \mathbb{K}^n$ .

Soit  $Y = \begin{bmatrix} y_1 \\ \dots \\ y_n \end{bmatrix} \in \mathcal{M}_{n,1}(\mathbb{K})$ . Étudions l'équation  $DX = Y$  d'inconnue  $X = \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix} \in \mathcal{M}_{n,1}(\mathbb{K})$ .

$$DX = Y \iff \begin{cases} d_1 x_1 & = & y_1 \\ & d_2 x_2 & = & y_2 \\ & & \ddots & = & \ddots \\ & & & d_n x_n & = & y_n \end{cases}$$

- Si  $\exists i_0 \in \llbracket 1; n \rrbracket : d_{i_0} = 0$ , la  $i_0$ -ème ligne du système ci-dessus devient une condition de compatibilité  $0 = y_{i_0}$  qui ne sera pas respecté pour  $Y = E^{i_0,1}$ . Donc  $D \notin \mathcal{GL}_n(\mathbb{K})$ .
- Sinon  $\forall i \in \llbracket 1; n \rrbracket : d_i \neq 0$ , le système est donc triangulaire à coefficients diagonaux non nuls. Il admet donc une unique solution. Ainsi  $D \in \mathcal{GL}_n(\mathbb{K})$ .

$$DX = Y \iff \begin{cases} x_1 & = & d_1^{-1} y_1 \\ & x_2 & = & d_2^{-1} y_2 \\ & & \ddots & = & \ddots \\ & & & x_n & = & d_n^{-1} y_n \end{cases}$$

Ainsi  $D^{-1} = \text{diag}(d_1^{-1}, d_2^{-1}, \dots, d_n^{-1})$ . □

## 20 Semaine 20

### 20.1 Éléments inversibles de l'anneau $\mathbb{K}[X]$

$$\mathbb{K}[X]^\times = \{\lambda X^0, \lambda \in \mathbb{K}^*\} \quad (26)$$

*Démonstration.* Soit  $P$  un élément inversible de  $\mathbb{K}[X]$ . Alors  $\exists Q \in \mathbb{K}[X] : P \cdot Q = Q \cdot P = 1_{\mathbb{K}[X]}$ . En prenant les degrés des polynômes,  $\deg P + \deg Q = 0$ .

Or  $\deg : \mathbb{K}[X] \rightarrow \mathbb{N}$  donc  $\deg P = \deg Q = 0$ . Donc  $\exists \lambda \in \mathbb{K}^* : P = \lambda$ .

Ainsi  $\mathbb{K}[X]^\times \subset \{\lambda X^0, \lambda \in \mathbb{K}^*\}$ .

Soit  $\lambda \in \mathbb{K}^*$ . Considérons  $P = \lambda$ . Posons  $Q = \lambda^{-1}$  (car  $\mathbb{K}$  est un corps).  $P \cdot Q = \lambda \lambda^{-1} = 1$  et  $Q \cdot P = \lambda^{-1} \lambda = 1$  donc  $P$  est inversible. Ainsi  $\{\lambda X^0, \lambda \in \mathbb{K}^*\} \subset \mathbb{K}[X]^\times$ .  $\square$

### 20.2 Théorème d'interpolation de Lagrange

Le problème d'interpolation de Lagrange est, pour  $n \in \mathbb{N}$  avec  $a \in \mathbb{K}^{n+1}$  et  $b \in \mathbb{K}^{n+1}$ , l'ensemble des polynômes passant par tous les points de coordonnée  $(a_i, b_i)$ . C'est-à-dire l'ensemble des  $P \in \mathbb{K}[X]$  vérifiant :

$$\forall i \in \llbracket 0; n \rrbracket, P(a_i) = b_i \quad (27)$$

Il existe une unique solution  $P$  de degré  $\leq n$  au problème d'interpolation de Lagrange, et elle s'exprime de la manière suivante en posant

$$L_i = \prod_{\substack{j=0 \\ j \neq i}}^n \frac{X - a_j}{a_i - a_j} \quad (28)$$

$$P = \sum_{i=0}^n b_i L_i \quad (29)$$

*Démonstration.* — Unicité

Supposons qu'il existe  $(P, Q) \in \mathbb{K}_n[X]^2$  solutions du problème d'interpolation.

Alors  $\forall i \in \llbracket 0, n \rrbracket, \tilde{P}(a_i) = \tilde{Q}(a_i) = b_i$

Posons  $H = P - Q$ , alors,  $\forall i \in \llbracket 0, n \rrbracket, \tilde{H}(a_i) = \tilde{P}(a_i) - \tilde{Q}(a_i) = 0$ .

De plus,  $\deg H = \deg(P - Q) \leq \max\{\deg P, \deg Q\}$

Donc  $H$  est un polynôme de degré  $\leq n$  avec  $|\llbracket 0, n \rrbracket| = n + 1$  racines.

Donc  $H$  est le polynôme nul.

— Existence Soit  $i \in \llbracket 0, n \rrbracket$  fq Notons  $L_i$  une solution de degré  $\leq n$  au problème  $Pb_i$  suivant :

$$(Pb_i) \left\{ \begin{array}{l} \tilde{P}(a_0) = 0 \\ \vdots \\ \tilde{P}(a_{i-1}) = 0 \\ \tilde{P}(a_i) = 1 \\ \tilde{P}(a_n) = 0 \\ \vdots \\ \tilde{P}(a_n) = 0 \end{array} \right.$$

On remarque que  $(a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$  sont  $n$  racines deux à deux distinctes de  $L_i$ . Or  $L_i$  est de degré  $\leq n$  et n'est pas le polynôme nul (car  $\tilde{L}_i(a_i) = 0$ ) donc  $(a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$  sont les *seules* racines de  $L_i$ , toutes simples.

Dès lors,

$$\exists c \in \mathbb{K}^* : L_i = c \prod_{\substack{j=0 \\ j \neq i}}^n (X - a_j)$$

Pour trouver le  $c$ , remarquons que

$$\begin{aligned}\tilde{L}_i(a_i) = 1 &\iff c \prod_{\substack{j=0 \\ j \neq i}}^n (a_i - a_j) = 1 \\ &\iff c = \prod_{\substack{j=0 \\ j \neq i}}^n \left( \frac{1}{a_i - a_j} \right)\end{aligned}$$

Ainsi, s'il existe une solution au problème  $Pb_i$  c'est nécessairement

$$L_i = \prod_{\substack{j=0 \\ j \neq i}}^n \left( \frac{X - a_j}{a_i - a_j} \right)$$

Réciproquement, cette solution est correcte puisque

$$\forall k \in \llbracket 0, n \rrbracket, k \neq i, \tilde{L}_i(a_k) = \prod_{\substack{j=0 \\ j \neq i}}^n \left( \frac{\overbrace{a_k - a_j}^{=0}}{a_i - a_j} \right) = 0$$

Et

$$\tilde{L}_i(a_i) = \prod_{\substack{j=0 \\ j \neq i}}^n \left( \frac{a_i - a_j}{a_i - a_j} \right) = \prod_{\substack{j=0 \\ j \neq i}}^n 1 = 1$$

Posons donc  $P = \sum_{i=0}^n b_i L_i$ .

Alors, par construction,

$$\forall k \in \llbracket 0, n \rrbracket, \tilde{P}(a_k) = \sum_{i=0}^n \left( b_i \prod_{\substack{j=0 \\ j \neq i}}^n \left( \frac{a_k - a_j}{a_i - a_j} \right) \right) = \sum_{i=0}^n (b_i \delta_{ki}) = b_k \delta_{kk} = b_k$$

Nous avons donc construit une solution unique au problème d'interpolation de Lagrange  $\square$

### 20.3 Formule de Taylor dans $\mathbb{K}[X]$ (caractéristique nulle)

Soient  $P$  à coefficients dans  $\mathbb{K}$  et  $a \in \mathbb{K}$ . On a :

$$P = \sum_{n \in \mathbb{N}} \frac{\widetilde{P^{(n)}}(a)}{n!} (X - a)^n \quad (30)$$

*Démonstration.* Considérons le prédicat  $\mathcal{P}(\cdot)$  défini sur  $\mathbb{N}$  par :

$$\mathcal{P}(n) : \text{ " } \forall P \in \mathbb{K}_n[X], P = \sum_{k=0}^n \frac{\widetilde{P^{(k)}}(a)}{k!} (X - a)^k \text{ "}$$

Initialisation : pour  $n = 0$ , soit  $P \in \mathbb{K}_0[X]$ .

$\exists p_0 \in \mathbb{K} : P = p_0 X^0$  et  $\sum_{k=0}^0 \frac{\widetilde{P^{(k)}}(a)}{k!} (X - a)^k = \frac{\widetilde{P^{(0)}}(a)}{1} X^0 = p_0 X^0$ , donc  $\mathcal{P}(0)$  vrai.

Hérédité : Soit  $n \in \mathbb{N}$  tel que  $\mathcal{P}(n)$ . Soit  $P \in \mathbb{K}_{n+1}[X]$ . On a donc  $\deg P' = \deg P - 1 \leq n$  donc  $\mathcal{P}(n)$  s'applique à  $P'$  :

$$P' = \sum_{k=0}^n \frac{\widetilde{P'^{(k)}}(a)}{k!} (X - a)^k = \left( \sum_{k=0}^n \frac{\widetilde{P^{(k+1)}}(a)}{k!} \frac{(X - a)^{k+1}}{k+1} \right)',$$

donc :

$$\left( P - \sum_{k=0}^n \frac{\widetilde{P^{(k+1)}}(a)}{k!} \frac{(X-a)^{k+1}}{k+1} \right)' = 0 \implies \exists \mu \in \mathbb{K} : P - \sum_{k=0}^n \frac{\widetilde{P^{(k+1)}}(a)}{k!} \frac{(X-a)^{k+1}}{k+1} = \mu,$$

ainsi :

$$P = \sum_{k=0}^n \frac{\widetilde{P^{(k+1)}}(a)}{(k+1)!} (X-a)^{k+1} + \mu = \sum_{k=1}^{n+1} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k + \mu,$$

donc en  $a$  par  $\varphi_a$  :

$$\widetilde{P}(a) = \mu \implies P = \sum_{k=1}^{n+1} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k + \widetilde{P}(a) = \sum_{k=0}^{n+1} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k,$$

donc  $\mathcal{P}(n+1)$  vrai. Ainsi par théorème de récurrence sur  $\mathbb{N}$ ,  $\mathcal{P}(n)$  est vrai pour tout  $n \in \mathbb{N}$ .  $\square$

## 20.4 Caractérisation de la multiplicité d'une racine

Soit  $P \in \mathbb{K}[X]$ . Soit  $a \in \mathbb{K}$ .

$$a \text{ est une racine de } P \text{ de multiplicité au moins } m \iff \begin{cases} P(a) = 0 \\ P'(a) = 0 \\ \vdots \\ P^{(m-1)}(a) = 0 \end{cases} \quad (31)$$

$$a \text{ est une racine de } P \text{ de multiplicité d'exactly } m \iff \begin{cases} P(a) = 0 \\ P'(a) = 0 \\ \vdots \\ P^{(m-1)}(a) = 0 \\ P^m(a) \neq 0 \end{cases} \quad (32)$$

*Démonstration.* • Supposons que  $a$  est une racine de  $P$  de multiplicité au moins  $m$ .

Alors  $\exists Q \in \mathbb{K}[X] : P = (X-a)^m Q$ . D'après la formule de Leibniz, pour tout  $k \in \llbracket 0; m-1 \rrbracket$ ,

$$\begin{aligned} P^{(k)} &= \sum_{i=0}^k \binom{k}{i} ((X-a)^m)^{(k-i)} Q^{(i)} \\ &= \sum_{i=0}^k \binom{k}{i} \frac{m!}{(m-(k-i))!} (X-a)^{m-(k-i)} Q^{(i)} \\ &= \underbrace{(X-a)^{(m-k)}}_{\substack{\text{c'est un bien un polynôme} \\ \text{non constant car } k < m}} \sum_{i=0}^k \binom{k}{i} \frac{m!}{(m-(k-i))!} (X-a)^i Q^{(i)} \end{aligned}$$

Donc  $\forall k \in \llbracket 0; m-1 \rrbracket, P^{(k)}(a) = 0$ .

- Supposons que  $\forall k \in \llbracket 0; m-1 \rrbracket, P^{(k)}(a) = 0$ .

Appliquons la formule de Taylor a.

$$\begin{aligned} P &= \sum_{n \in \mathbb{N}} \frac{P^{(n)}(a)}{n!} (X-a)^n \\ &= \sum_{n=0}^{m-1} \underbrace{\frac{P^{(n)}(a)}{n!}}_{=0} (X-a)^n + \sum_{\substack{n \in \mathbb{N} \\ n \geq m}} \frac{P^{(n)}(a)}{n!} (X-a)^n \\ &= (X-a)^m \sum_{\substack{n \in \mathbb{N} \\ n \geq m}} \frac{P^{(n)}(a)}{n!} \underbrace{(X-a)^{n-m}}_{\in \mathbb{K}[X] \text{ car } n-m \in \mathbb{N}} \end{aligned}$$

Donc  $(X-a)^m | P$ . Donc  $a$  est racine de  $P$  de multiplicité au moins  $m$ .

- Supposons que  $a$  est une racine de  $P$  de multiplicité exactement  $m$ .  
Nous pouvons appliquer le point précédent car la multiplicité est supérieur à  $m : \forall k \in \llbracket 0; m-1 \rrbracket, P^{(k)}(a) = 0$ .  
Par l'absurde, si  $P^{(m)}(a) = 0$  alors le point précédent donne que  $a$  a une multiplicité supérieur à  $m+1$  donc  $m \geq m+1$  ce qui est une contradiction.  
Par conséquent,  $P^{(m)}(a) \neq 0$ .
- Supposons  $\forall k \in \llbracket 0; m-1 \rrbracket, P^{(k)}(a) = 0$  et  $P^{(m)}(a) \neq 0$ .  
En reprenant le calcul précédent, pour  $k = m$ , en sachant que  $(X-a)^{(m-k)} = X^0$ ,

$$P^{(m)} = \binom{m}{0} \frac{m!}{0!} (X-a)^0 P + \sum_{i=1}^m \binom{m}{i} \frac{m!}{i!} (X-a)^i Q^{(i)}$$

D'où  $P^{(m)}(a) = m! Q(a)$  donc  $Q(a) = \frac{P^{(m)}(a)}{m!}$ . Donc  $Q(a) \neq 0$ .

Par l'absurde, supposons que  $(X-a)^{m+1} | P$ . Alors  $\exists R \in \mathbb{K}[X] : P = (X-a)^{m+1} R$ . Donc  $(X-a)^{m+1} R = (X-a)^m Q$  d'où  $Q = (X-a)R$ . Nous obtenons  $Q(a) = 0$  ce qui est une contradiction avec  $Q(a) \neq 0$ .

Donc  $a$  est une racine de  $P$  de multiplicité strictement inférieur à  $m+1$  et, d'après le point précédent, supérieur à  $m$ . Donc  $a$  est une racine de  $P$  de multiplicité exactement  $m$ .  $\square$

## 20.5 Identification de $\mathbb{K}[X]$ à $\mathbb{K}[x]$ , par l'injectivité de $\Phi$

*Démonstration.* Montrons que l'application  $\Phi$  définie comme suit est injective :

$$\Phi : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathcal{F}(\mathbb{K}, \mathbb{K}) \\ P & \longmapsto & \tilde{P} \end{array} \right. .$$

Soit donc  $P \in \ker \Phi$ , on a :

$$\Phi(P) = \tilde{0} \implies \tilde{P} = \tilde{0} \text{ sur } \mathbb{K} \implies P = 0_{\mathbb{K}[X]},$$

donc  $\ker \Phi \subset \{0_{\mathbb{K}[X]}\}$ .

Réciproquement, on calcule l'image du polynôme nul par  $\Phi$  :

$$\Phi(0_{\mathbb{K}[X]}) = \tilde{0},$$

donc  $0_{\mathbb{K}[X]} \in \ker \Phi$ , ainsi on a l'égalité ensembliste et donc cela suffit.  $\square$

## 20.6 Pour $P = (X-x_1)(X-x_2)(X-x_3)$ , exprimer $x_1^3 + x_2^3 + x_3^3$ en fonction des fonctions symétriques élémentaires

Les fonctions symétriques élémentaires  $(\sigma_k)_{k \in \llbracket 0; n \rrbracket}$  pour une famille  $(x_k)_{k \in \llbracket 1; n \rrbracket}$  sont définies par

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} \prod_{j=1}^k x_{i_j} \quad (33)$$

*Démonstration.* Sous forme développée,  $P = X^3 - (x_1 + x_2 + x_3)X^2 + (x_1x_2 + x_1x_3 + x_2x_3)X - x_1x_2x_3 = X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$ . Comme  $x_1, x_2, x_3$  sont racines de  $P$ , nous avons les trois égalités suivantes :

$$0 = P(x_1) = x_1^3 - \sigma_1 x_1^2 + \sigma_2 x_1 - \sigma_3$$

$$0 = P(x_2) = x_2^3 - \sigma_1 x_2^2 + \sigma_2 x_2 - \sigma_3$$

$$0 = P(x_3) = x_3^3 - \sigma_1 x_3^2 + \sigma_2 x_3 - \sigma_3$$

En sommant ces trois équation,

$$0 = x_1^3 + x_2^3 + x_3^3 - \sigma_1(x_1^2 + x_2^2 + x_3^2) + \sigma_2(x_1 + x_2 + x_3) - 3\sigma_3$$

Cherchons la somme des carrés.

$$\begin{aligned} (x_1 + x_2 + x_3)^2 &= x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3 \\ \implies x_1^2 + x_2^2 + x_3^2 + x_1x_2 &= \sigma_1^2 - 2\sigma_2 \end{aligned}$$

Ainsi

$$x_1^3 + x_2^3 + x_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

$\square$

## 20.7 Expression de $S_2$ , $S_{-1}$ et $S_{-2}$ à l'aide des fonctions élémentaires symétriques.

Les sommes de Newton  $(S_k)_{k \in \mathbb{Z}^*}$  pour une famille  $(x_k)_{k \in \mathbb{N}^*}$  sont définies par (sous réserve d'existence pour  $k < 0$ ) :

$$S_k = \sum_{i=1}^n x_i^k \quad (34)$$

*Démonstration.*

$$\begin{aligned} \sigma_1^2 &= \left( \sum_{i=1}^n x_i \right)^2 \\ &= \underbrace{\sum_{i=1}^n x_i^2}_{S_2} + 2 \underbrace{\sum_{1 \leq i < j \leq n} x_i x_j}_{\sigma_2} \\ \implies S_2 &= \sigma_1^2 - 2\sigma_2 \\ S_{-1} &= \sum_{i=1}^n \frac{1}{x_i} = \frac{\sum_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n x_j}{\prod_{i=1}^n x_i} = \frac{\sigma_{n-1}}{\sigma_n} \\ S_{-2} &= \sum_{i=1}^n \frac{1}{x_i^2} \\ &= \left( \sum_{i=1}^n \frac{1}{x_i} \right)^2 - 2 \sum_{1 \leq i < j \leq n} \frac{1}{x_i} \frac{1}{x_j} \\ &= \frac{\sigma_{n-1}^2}{\sigma_n^2} - 2 \frac{\sum_{1 \leq i < j \leq n} \prod_{\substack{k=1 \\ k \notin \{i,j\}}}^n \frac{1}{x_k}}{\sigma_n} \\ &= \frac{\sigma_{n-1}^2 - 2\sigma_{n-2}\sigma_n}{\sigma_n^2} \end{aligned}$$

□



## 21 Semaine 21

### 21.1 Caractérisation des polynômes irréductibles de degré 1, 2 et 3 dans $\mathbb{K}[X]$ .

Tous les polynômes de degré 1 sont irréductibles, les polynômes irréductibles de degré 2 ou 3 sont les polynômes sans racine.s dans le corps de base.

*Démonstration.* Un polynôme de degré 1 ne peut s'écrire comme produit de 2 polynômes de degré  $\geq 1$  donc il est irréductible.

Soit  $P \in \mathbb{K}[X]$  un polynôme irréductible de degré 2 ou 3.

Par définition,  $P$  n'a pas de racine.s dans  $\mathbb{K}$ , donc la première inclusion.

Soit  $P \in \mathbb{K}[X]$  tel que  $\deg P = 2$ .

Montrons que si  $P$  n'a pas de racine dans  $\mathbb{K}$  alors  $P$  est irréductible. Montrons la contraposée. Supposons  $P$  non-irréductible.

$$\exists A, B \in \mathbb{K}[X] : P = AB \text{ et } \deg A, \deg B \geq 1,$$

On a alors,  $P = AB \implies 2 = \deg A + \deg B \implies \deg A, \deg B = 1$  donc :

$$\exists \alpha, \gamma \in \mathbb{K}^* \times \mathbb{K} : A = \alpha X + \gamma,$$

ainsi,  $P = (\alpha X + \gamma)B = \alpha \left(X + \frac{\gamma}{\alpha}\right) B$ , donc  $P$  admet  $-\frac{\gamma}{\alpha} \in \mathbb{K}$  comme racine, ce qui montre la contraposée.

Soit  $P \in \mathbb{K}[X]$  tel que  $\deg P = 3$ .

Montrons, de même, la contraposée. Supposons  $P$  non-irréductible. De même, on a :

$$\exists A, B \in \mathbb{K}[X] : P = AB \text{ et } \deg A, \deg B \geq 1,$$

Puis encore,  $P = AB \implies 3 = \deg A + \deg B \implies \deg A, \deg B \in \{2, 1\}$  (l'un n'étant pas l'autre). Donc l'un des deux est de degré 1 donc  $P$  admet une racine dans  $\mathbb{K}$ , donc encore une fois cela montre la contraposée, ce qui démontre l'inclusion réciproque.  $\square$

### 21.2 Polynômes irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$ .

Les polynômes irréductibles de  $\mathbb{C}[X]$  sont les polynômes de degré 1 et ceux de  $\mathbb{R}[X]$  sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.

*Démonstration.* Le premier point est immédiat, les polynômes irréductibles d'un corps contiennent les polynômes de degré 1 et par le théorème de D'Alembert-Gauss, tout polynôme de  $\mathbb{C}[X]$  ( $\deg \geq 2$ ) est scindé dans  $\mathbb{C}[X]$ , donc non-irréductible.

Pour le second point, le cas du degré 1 est réglé. Soit  $P$  un polynôme irréductible de  $\mathbb{R}[X]$ .

Supposons que  $P$  soit de degré supérieur ou égal à 3. Si son degré est impair, le TVI conclut quant à l'existence d'une racine, donc non-irréductible. Si son degré est pair, par D'Alembert-Gauss, on obtient  $\deg P$  couples de racines possiblement égaux.

Or,  $P \in \mathbb{R}[X]$  donc  $\forall z \in \mathbb{C}, P(z) = 0 \implies P(\bar{z}) = 0$  donc les racines se rassemblent 2 à 2 pour former un polynôme scindé dans  $\mathbb{R}$ , donc non-irréductible. Ainsi,  $\deg P = 2$ , immédiatement, si le discriminant de  $P$  est positif ou nul,  $P$  admet une ou deux racines dans  $\mathbb{R}$ , donc non irréductible. Enfin, son discriminant est alors négatif, de cette manière  $P$  n'admet pas de racine dans  $\mathbb{R}$  et est donc irréductible. Ce qui achève la preuve.  $\square$

### 21.3 $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$ .

Il s'agit donc de montrer que racine cubique de 2 n'est pas un rationnel.

*Démonstration.* Supposons, par l'absurde, qu'il existe  $r \in \mathbb{Q}$  tel que  $r^3 - 2 = 0$ . Prenons  $p, q \in \mathbb{Z} \times \mathbb{N}^*$  le représentant irréductible de  $r$  dans  $\mathbb{Q}$ . On a alors,  $p^3 = 2q^3$  donc  $2 \mid p^3$  or  $2 \in \mathcal{P}$  donc  $2 \mid p$ , ainsi, il existe  $k \in \mathbb{Z}$  tel que  $p = 2k$ . Par conséquent,  $2(2k^3) = q^3$  donc  $2 \mid q^3$  or  $2 \in \mathcal{P}$  donc  $2 \mid q$  donc ceci contredit  $p$  et  $q$  premiers entre eux, par définition d'un représentant irréductible. Ainsi,  $P = X^3 - 2$  n'admet pas de racine dans  $\mathbb{Q}$ , c'est donc un polynôme irréductible.  $\square$

## 21.4 PGCD d'un polynôme de $\mathbb{C}[X]$ et son polynôme dérivé

Pour  $P = \prod_{k=1}^p (X - z_k)^{m_k} \in \mathbb{C}[X] \setminus \{0_{\mathbb{C}[X]}\}$  avec  $m_k \in \mathbb{N}^*$  pour tout  $k \in \llbracket 1, p \rrbracket$ , on a

$$P \wedge P' = \prod_{k=1}^p (X - z_k)^{m_k - 1} \quad (35)$$

C'est une conséquence de la définition du pgcd de deux polynômes  $P \wedge Q = \prod_{i \in I} P_i^{\min\{m_i, p_i\}}$ , où les  $P_i$  sont les facteurs irréductibles de  $P$  et  $Q$  dans leur décomposition.

*Démonstration.* Soit  $P$  un tel polynôme et  $p$  un entier naturel non nul. Naturellement,  $P'$  hérite de  $P$ ,  $\deg P - p$  racines, lesquelles sont les  $z_k$  pour  $k \in \llbracket 1, p \rrbracket$ , de multiplicité  $m_k - 1$ . Ainsi,

$$\exists B \in \mathbb{C}[X] : \left[ P' = \left( \prod_{k=1}^p (X - z_k)^{m_k - 1} \right) B \right] \wedge [\deg B = p],$$

de cette manière on peut écrire :

$$P' = \left( \left( \prod_{k=1}^p (X - z_k)^{m_k - 1} \right) B \right) P^0 \text{ et } P = \left( \prod_{k=1}^p (X - z_k)^{m_k} \right) (P')^0,$$

de façon à faire apparaître dans les deux décompositions les mêmes facteurs, possiblement avec une puissance 0, histoire de coller à la définition de manière explicite. Ceci fait, il ne reste plus qu'à appliquer la définition du pgcd et de remarquer que seuls les  $(X - z_k)^{m_k - 1}$  subsistent.

Notons  $\mathfrak{J}$  l'ensemble des facteurs de leur décomposition, on a alors :

$$P \wedge P' = \prod_{D \in \mathfrak{J}} D^{\min\{\nu_D(P), \nu_D(P')\}} = \prod_{k=1}^p (X - z_k)^{m_k - 1},$$

où  $\nu_D(\cdot)$  est la valuation  $D$ -adique au sens des polynômes irréductibles. Ce qui conclut.  $\square$

## 21.5 Justifier la bonne définition de la dérivée d'une fraction rationnelle.

Il s'agit là de vérifier que la définition que l'on souhaiterait le plus, c'est-à-dire la même que pour la dérivée d'une fraction de fonctions, s'applique effectivement aux fractions rationnelles, c'est-à-dire que cette définition ne dépend pas du représentant choisi.

*Démonstration.* Montrons que pour  $A, B \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ , on a :

$$\left( \frac{A}{B} \right)' = \frac{A'B - B'A}{B^2}.$$

Soient  $A$  et  $B$  de tels polynômes et  $C, D \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$  tels que  $AD = BC$ , en dérivant on obtient  $A'D + D'A = B'C + C'B$ . Calculons :

$$\begin{aligned} (A'B - B'A)D^2 &= D(A'BD - (AD)B') \\ &= D(A'BD - BCB') \\ &= BD(A'D - CB') \\ &= BD(C'B - D'A) \\ &= B(C'BD - (AD)D') \\ &= B(C'BD - BCD') \\ &= B^2(C'D - D'C), \end{aligned}$$

ce qui prouve que le résultat ne dépend pas du représentant, par définition de  $\mathbb{K}(X)$  comme structure quotient.  $\square$

## 21.6 Théorème de Gauss-Lucas et interprétation graphique.

Les racines du polynôme dérivée sont dans l'enveloppe convexe des racines du polynôme.  
Soit  $P \in \mathbb{C}[X]$  de degré au moins 2 et notons  $z_1, \dots, z_n$  ses racines répétées avec multiplicité.  
Soit  $u$  une racine de  $P'$ . Alors :

$$\exists (c_1, \dots, c_n) \in \mathbb{R}_+^* : \sum_{k=1}^n c_k z_k = u \text{ et } \sum_{k=1}^n c_k = 1. \quad (36)$$

*Démonstration.* Pour ce qui est de l'interprétation graphique, elle n'est pas prévue à l'heure qu'il est dans ce pdf, pour la faire soi-même dessiner des points et les "clôturer" dans un polygone convexe, ou même faire ceci avec un cas concret.

→ Si  $u$  est une racine de  $P$  alors noter  $k_0$  son indice et utiliser le symbole de Kronecker.

$$\sum_{k=1}^n \delta_{k,k_0} z_k = u \text{ et } \sum_{k=1}^n \delta_{k,k_0} = 1.$$

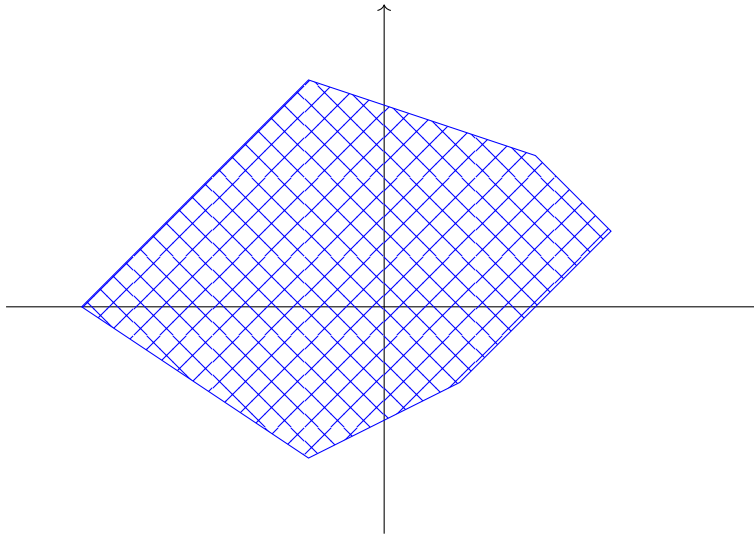
→ Sinon,  $u$  n'appartient pas aux racines de  $P$ , donc  $u$  n'est pas pôle de  $\frac{P'}{P}$  ce qui permet de prendre l'image par le morphisme d'évaluation en  $u$  de cette même fraction rationnelle :

$$0_{\mathbb{K}} = \frac{P'(u)}{P(u)} = \sum_{k=1}^n \frac{1}{u - z_k} = \sum_{k=1}^n \frac{\bar{u} - \bar{z}_k}{|u - z_k|^2} = \sum_{k=1}^n \frac{\bar{u}}{|u - z_k|^2} - \sum_{k=1}^n \frac{\bar{z}_k}{|u - z_k|^2}.$$

Donc en passant la seconde somme à gauche et en prenant le conjugué :

$$\sum_{k=1}^n \frac{u}{|u - z_k|^2} = \sum_{k=1}^n \frac{z_k}{|u - z_k|^2} \implies u = \frac{\sum_{k=1}^n \frac{z_k}{|u - z_k|^2}}{\sum_{k=1}^n \frac{1}{|u - z_k|^2}} = \sum_{k=1}^n \underbrace{\frac{\frac{1}{|u - z_k|^2}}{\sum_{i=1}^n \frac{1}{|u - z_i|^2}}}_{= c_k} z_k = \sum_{k=1}^n c_k z_k,$$

ce qui démontre la première partie du résultat, il est immédiat de vérifier que  $\sum_{k=1}^n c_k = 1$ , vérification laissée aux lecteurs. Ce qui achève la preuve.



$$P = (X + 4)^3(X + 1 - 3i)(X - 2 - 2i)^2(X - 3 - i)(X - 1 + i)(X + 1 + 2i)^2$$

Les racines de  $P'$  sont dans le polygone bleu.

□

## 21.7 Deux expressions du coefficient associé à un pôle simple dans une décomposition en éléments simples.

*Démonstration.* Soient  $(P, Q) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\})$  tels que la fraction rationnelle  $\frac{P}{Q}$  soit irréductible et en prenant  $\deg P < \deg Q$ . En appliquant le théorème de décomposition en éléments simples, on obtient une expression de la forme :

$$\exists R \in \mathbb{K}(X) : \frac{P}{Q} = \sum_{k=1}^n \frac{a_k}{X - z_k} + R,$$

où les  $z_k$  pour  $k \in \llbracket 1, n \rrbracket$  sont racines de  $Q$ . Ainsi, en prenant  $k_0 \in \llbracket 1, n \rrbracket$  tel que  $z_{k_0}$  soit racine simple,

$$\frac{P(X - z_{k_0})}{Q} = a_{k_0} + \sum_{k=0 \text{ et } k \neq k_0} \frac{a_k(X - z_{k_0})}{X - z_{k_0}} + R(X - z_{k_0}),$$

une première expression se trouvera en notant  $\tilde{Q} = \prod_{\substack{k=1 \\ k \neq k_0}}^n (X - z_k)^{\nu_{(X-z_k)}(Q)}$ , on a alors :

$$\frac{P(z_{k_0})}{\tilde{Q}(z_{k_0})} = a_{k_0}.$$

Une autre expression est possible en explicitant  $\tilde{Q}$ . Pour ce faire, remarquons plutôt :

$$Q' = \sum_{k=1}^n \nu_{(X-z_k)}(Q) (X - z_k)^{\nu_{(X-z_k)}(Q)-1} \prod_{\substack{i=1 \\ i \neq k}}^n (X - z_i)^{\nu_{(X-z_i)}(Q)},$$

donc en prenant l'image par le morphisme d'évaluation en  $z_{k_0}$  on obtient :

$$Q'(z_{k_0}) = \prod_{\substack{i=1 \\ i \neq k_0}}^n (z_{k_0} - z_i)^{\nu_{(X-z_i)}(Q)},$$

il s'agit exactement de  $\tilde{Q}(z_{k_0})$ . Ainsi,

$$\frac{P(z_{k_0})}{Q'(z_{k_0})} = a_{k_0}, \quad (37)$$

ce qui suffit.  $\square$

## 21.8 Expressions des deux coefficients associés à un pôle double dans une décomposition en éléments simples.

*Démonstration.* Soient  $(P, Q) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\})$  tels que la fraction rationnelle  $\frac{P}{Q}$  soit irréductible et en prenant  $\deg P < \deg Q$ . En appliquant le théorème de décomposition en éléments simples on obtient une expression de la forme suivante en considérant  $z_{k_0}$ , une racine double de  $Q$  :

$$\exists R \in \mathbb{K}(X) : \frac{P}{Q} = \frac{a_1}{X - z_{k_0}} + \frac{a_2}{(X - z_{k_0})^2} + R \quad (\star)$$

puis de même,

$$\frac{P(X - z_{k_0})}{Q} = a_2 + \left( \frac{a_1}{X - z_{k_0}} + R \right) (X - z_{k_0})^2,$$

donc en notant  $\tilde{Q} = \prod_{\substack{k=1 \\ k \neq k_0}}^n (X - z_k)^{\nu_{(X-z_k)}(Q)}$ , on a :

$$\frac{P(z_{k_0})}{\tilde{Q}(z_{k_0})} = a_2,$$

c'est une première expression. Pour la suivante, encore une fois, explicitons  $\tilde{Q}$ . Remarquons que :

$$\exists A \in \mathbb{K}[X] : \left[ Q'' = 2 \prod_{\substack{k=1 \\ k \neq k_0}}^n (X - z_k)^{\nu_{(X-z_k)}(Q)} + A \right] \wedge [A(z_{k_0}) = 0],$$

donc, en remarquant que :

$$2\tilde{Q}(z_{k_0}) = Q''(z_{k_0}),$$

on a finalement :

$$\frac{2P(z_{k_0})}{Q''(z_{k_0})} = a_2.$$

Pour récupérer  $a_1$ , on multiplie  $(\star)$  par  $(X - z_{k_0})^2$  puis on dérive :

$$\left( \frac{P(X - z_{k_0})^2}{Q} \right)' = a_1 + R'(X - z_{k_0})^2 + 2R(X - z_{k_0}),$$

soit,

$$\frac{((P'(X - z_{k_0})^2 + 2P(X - z_{k_0}))Q - Q'P(X - z_{k_0})^2)}{Q^2} = a_1 + R'(X - z_{k_0})^2 + 2R(X - z_{k_0})$$

□

## 22 Semaine 22

Pour cette semaine,  $\mathbb{K}$  désigne un corps commutatif,  $E$  et  $F$  des  $\mathbb{K}$ -espaces vectoriels,  $E'$  et  $F'$  des sous-espaces vectoriels respectivement de  $E$  et de  $F$ ,  $I$  un ensemble quelconque non vide.

### 22.1 Caractérisation d'une famille liée

Une famille est liée si et seulement si l'un de ses vecteurs est une combinaison linéaire d'autres vecteurs de la famille.

$$(x_i)_{i \in I} \text{ est liée } \iff \exists i_0 \in I : \exists (\lambda_i)_{i \in I \setminus \{i_0\}} \in \mathbb{K}^{(I \setminus \{i_0\})} : x_{i_0} = \sum_{\substack{i \in I \\ i \neq i_0}} \lambda_i \cdot x_i \quad (38)$$

*Démonstration.* Supposons que  $(x_i)_{i \in I}$  est liée.

Par définition,  $\exists (\mu_i)_{i \in I} \in \mathbb{K}^{(I)} : \begin{cases} \sum_{i \in I} \mu_i x_i = 0_E \\ (\mu_i)_{i \in I} \neq (0_{\mathbb{K}})_{i \in I} \end{cases}$

Donc  $\exists i_0 \in I : \mu_{i_0} \neq 0_{\mathbb{K}}$ . Fixons un tel  $i_0$ .

$$\mu_{i_0} x_{i_0} + \sum_{i \in I \setminus \{i_0\}} \mu_i x_i = 0_E$$

$$\text{Or } \mu_{i_0} \neq 0, \text{ donc } x_{i_0} = \sum_{i \in I \setminus \{i_0\}} (\mu_{i_0}^{-1} \times (-\mu_i)) \cdot x_i.$$

$$\text{En posant } \lambda_i = \mu_{i_0}^{-1} \times (-\mu_i), \text{ on obtient } x_{i_0} = \sum_{i \in I \setminus \{i_0\}} \lambda_i \cdot x_i.$$

$$\text{Supposons maintenant que } \exists i_0 \in I : \exists (\lambda_i)_{i \in I \setminus \{i_0\}} \in \mathbb{K}^{(I \setminus \{i_0\})} : x_{i_0} = \sum_{\substack{i \in I \\ i \neq i_0}} \lambda_i \cdot x_i.$$

Alors  $-x_{i_0} + \sum_{\substack{i \in I \\ i \neq i_0}} \lambda_i \cdot x_i = 0_E$ . Posons  $\mu_{i_0} = -1_{\mathbb{K}}$  et  $\forall i \in I \setminus \{i_0\}, \mu_i = \lambda_i$ . Ainsi,  $(\mu_i)_{i \in I} \in \mathbb{K}^{(I)}$  et

$$\sum_{i \in I} \mu_i \cdot x_i = 0_{\mathbb{K}}.$$

Or  $\mu_{i_0} \neq 0_{\mathbb{K}}$  donc  $(\mu_i)_{i \in I} \neq (0_{\mathbb{K}})_{i \in I}$ .

Donc  $(\mu_i)_{i \in I}$  est liée. □

### 22.2 Caractérisations d'une base

Soit  $\mathcal{F}$  une famille de vecteurs de  $E$ . Les propositions suivantes sont équivalentes :

- (i)  $\mathcal{F}$  est une base.
- (ii) Tout vecteur de  $E$  se décompose de manière unique dans  $\mathcal{F}$ .
- (iii)  $\mathcal{F}$  est génératrice minimale (au sens de l'inclusion)
- (iv)  $\mathcal{F}$  est libre maximale (au sens de l'inclusion)

*Démonstration.* Notons  $(e_i)_{i \in I}$  la famille  $\mathcal{F}$ .

(i)  $\implies$  (ii) Supposons que  $\mathcal{F}$  est une base de  $E$ .

Soit  $x \in E$  fixé quelconque. Montrons que  $x$  s'écrit de manière unique comme une combinaison linéaire des vecteurs de  $\mathcal{F}$ .

$\mathcal{F}$  est une base donc elle est une famille génératrice et libre de  $E$ . La propriété génératrice donne, par définition, l'existence d'une telle écriture tandis que la propriété libre donne l'unicité d'une telle écriture.

(ii)  $\implies$  (iii) Supposons que tout vecteur de  $E$  s'écrit de manière unique comme une combinaison linéaire de vecteurs de  $\mathcal{F}$ .

L'existence d'une telle décomposition permet d'affirmer que  $\mathcal{F}$  est génératrice.

Supposons que  $\mathcal{F}$  ne soit pas génératrice minimale c'est-à-dire qu'il existe une famille  $\mathcal{F}'$  de vecteurs de  $E$  telle que  $\mathcal{F}' \subsetneq \mathcal{F}$  et  $\mathcal{F}'$  engendre  $E$ .

Alors  $\exists i_0 \in I : e_{i_0} \notin \mathcal{F}'$ . Comme  $\mathcal{F}'$  est génératrice,  $\exists (\lambda_i)_{i \in I \setminus \{i_0\}} \in \mathbb{K}^{(I \setminus \{i_0\})} : e_{i_0} = \sum_{\substack{i \in I \\ i \neq i_0}} \lambda_i \cdot e_i$ .

Donc

$$e_{i_0} = 0_{\mathbb{K}} \cdot e_{i_0} + \sum_{\substack{i \in I \\ i \neq i_0}} \lambda_i \cdot e_i$$

$$e_{i_0} = 1_{\mathbb{K}} \cdot e_{i_0} + \sum_{\substack{i \in I \\ i \neq i_0}} 0_{\mathbb{K}} \cdot e_i$$

$e_{i_0}$  peut donc s'écrire de deux manières différentes au moins comme combinaison linéaire de vecteurs de  $\mathcal{F}$  ce qui contredit le caractère libre de  $\mathcal{F}$ .

Par conséquent,  $\mathcal{F}$  est génératrice et minimale parmi les familles génératrices.

(iii)  $\implies$  (iv) Supposons que  $\mathcal{F}$  est une famille génératrice minimale. Par l'absurde, supposons que  $\mathcal{F}$  est liée. Alors il existe un  $i_0 \in I$  tel que  $e_{i_0}$  s'écrit comme une combinaison linéaire d'autres vecteurs de  $\mathcal{F}$  donc  $(e_i)_{i \in I \setminus \{i_0\}}$  est génératrice de  $E$ . Or cette famille est strictement incluse dans  $\mathcal{F}$  ce qui contredit la propriété de génératrice minimale.

Donc  $\mathcal{F}$  est libre.

Par l'absurde, supposons que  $\mathcal{F}$  n'est pas libre maximale c'est-à-dire qu'il existe une famille  $\mathcal{F}'$  de vecteurs de  $E$  telle que  $\mathcal{F} \subsetneq \mathcal{F}'$  et  $\mathcal{F}'$  est libre.

Alors  $\exists x \in \mathcal{F}' : x \notin \mathcal{F}$ . Or  $\mathcal{F}$  est génératrice d'où :

$$\exists (\lambda_i)_{i \in I} \in \mathbb{K}^{(I)} : x = \sum_{i \in I} \lambda_i \cdot x_i = 0_{\mathbb{K}} \cdot x + \sum_{i \in I} \lambda_i \cdot x_i + \sum_{\substack{y \in \mathcal{F}' \\ y \notin \mathcal{F} \\ y \neq x}} 0_{\mathbb{K}} \cdot y$$

Puisque  $x \in \mathcal{F}'$ ,

$$\exists (\lambda_i)_{i \in I} \in \mathbb{K}^{(I)} : x = 1_{\mathbb{K}} \cdot x + \sum_{i \in I} 0_{\mathbb{K}} \cdot x_i + \sum_{\substack{y \in \mathcal{F}' \\ y \notin \mathcal{F} \\ y \neq x}} 0_{\mathbb{K}} \cdot y$$

Donc  $x$  s'écrit de deux manières différentes au moins comme combinaison linéaire de vecteurs  $\mathcal{F}'$ , ce qui contredit la liberté de  $\mathcal{F}'$ .

Par conséquent,  $\mathcal{F}$  est libre maximale.

(iv)  $\implies$  (i) Supposons que  $\mathcal{F}$  est une famille libre maximale.

Par hypothèse même,  $\mathcal{F}$  est libre. Par l'absurde, supposons que  $\mathcal{F}$  n'est pas génératrice. Alors il existe  $x \in E$  tel que  $x \notin \text{Vect } \mathcal{F}$ . Donc  $\mathcal{F} \cup \{x\}$  est libre et contient strictement  $\mathcal{F}$ , ce qui contredit la propriété de liberté maximale.

Par conséquent,  $\mathcal{F}$  est aussi génératrice, donc une base.

$$\begin{array}{ccc} (i) & \implies & (ii) \\ \uparrow & & \downarrow \\ (iv) & \longleftarrow & (iii) \end{array}$$

□

## 22.3 Le noyau et l'image d'une application linéaire sont des sous-espaces vectoriels

Soit  $f \in \mathcal{L}_{\mathbb{K}}(E, F)$ .

$$\begin{aligned} \ker f &= \{x \in E \mid f(x) = 0_F\} = f^{-1}(\{0_F\}) \\ \text{Im } f &= \{y \in F \mid \exists x \in E : f(x) = y\} \end{aligned} \tag{39}$$

Nous démontrerons le résultat plus général suivant :

- (i)  $f(E')$  est un sous-espace vectoriel de  $F$ .
- (ii)  $f^{-1}(F')$  est un sous-espace vectoriel de  $E$ .

*Démonstration.* (i)  $0_E \in E'$  et  $f(0_E) = 0_F$  donc  $0_F \in f(E')$  d'où  $f(E') \neq \emptyset$

Soit  $(\alpha, \beta, y, y') \in \mathbb{K}^2 \times f(E')^2$  fixés quelconques.

Par définition,  $\exists (x, x') \in E'^2 : f(x) = y \wedge f(x') = y'$ .

$$\begin{aligned} \alpha y + \beta y' &= \alpha f(x) + \beta f(x') \\ &= f(\alpha x + \beta x') \quad \text{car } f \in \mathcal{L}_{\mathbb{K}}(E, F) \\ &\in f(E') \quad \text{car } \alpha x + \beta x' \in E' \text{ puisque } E' \text{ est un sous-espace vectoriel} \end{aligned}$$

Donc  $f(E')$  est un sous-espace vectoriel.

(ii)  $0_F \in F'$  et  $f(0_E) = 0_F$  donc  $0_E \in f^{-1}(F')$  d'où  $f^{-1}(F') \neq \emptyset$

Soit  $(\alpha, \beta, x, x') \in \mathbb{K}^2 \times f^{-1}(F')^2$  fixés quelconques.

Par définition,  $\exists (y, y') \in F'^2 : f(x) = y \wedge f(x') = y'$ .

Or  $F'$  est sous-espace vectoriel donc  $\alpha y + \beta y' \in F'$ .  $f \in \mathcal{L}_{\mathbb{K}}(E, F)$  d'où  $f(\alpha x + \beta x') = \alpha y + \beta y'$ .

Donc  $\alpha x + \beta x' \in f^{-1}(F')$ .

Ainsi,  $f^{-1}(F')$  est un sous-espace vectoriel.

En appliquant pour  $E' = E$  et  $F' = \{0_F\}$ , nous obtenons que  $\ker f$  et  $\text{Im} f$  sont des sous-espaces vectoriels.  $\square$

## 22.4 L'image par une application linéaire d'une partie génératrice engendre l'image de l'application linéaire

Soient  $(E, F)$  deux  $\mathbb{K}$ -espaces vectoriels  $f \in \mathcal{L}_{\mathbb{K}}(E, F)$ ,  $\mathcal{F} = (x_i)_{i \in I}$  une base de  $E$ .

Alors

$$\text{Vect } \underbrace{f(\mathcal{F})}_{\{f(x_i) | i \in I\}} = f(\text{Vect } \mathcal{F}) \quad (40)$$

*Démonstration.* Soit  $y \in \text{Vect } f(\mathcal{F})$  Alors  $\exists (\lambda_i)_{i \in I} \in \mathbb{K}^{(I)}$  tel que  $y = \sum_{i \in I} \lambda_i f(x_i)$  Mais

$$\begin{aligned} y &= \sum_{i \in I} \lambda_i f(x_i) \\ &= f\left(\sum_{i \in I} \lambda_i x_i\right) \implies y \in f(\text{Vect } \mathcal{F}) \end{aligned}$$

Réciproquement soit  $y \in f(\text{Vect } \mathcal{F})$  fq.

$$\exists x \in \text{Vect } \mathcal{F} : f(x) = y \implies \exists (x_i)_{i \in I} : x = \sum_{i \in I} \lambda_i x_i$$

Donc :

$$\begin{aligned} y = f(x) &= f\left(\sum_{i \in I} \lambda_i x_i\right) \\ &= \sum_{i \in I} \lambda_i f(x_i) \in \text{Vect } f(\mathcal{F}) \end{aligned}$$

$\square$

## 22.5 Caractérisation inj/surj/bij d'une application linéaire par l'image d'une base de l'espace de départ.

Nous donnerons les caractérisations au fur et à mesure de la démonstration.

*Démonstration.* Soient donc pour la suite,  $f \in \mathcal{L}_{\mathbb{K}}(E, F)$ ,  $\mathcal{B} = (e_i)_{i \in I}$  une base de  $E$ ,  $\mathcal{B}' = (e'_i)_{i \in I}$  une base de  $F$ ,  $\mathcal{F} = (x_i)_{i \in I}$  une famille libre de  $E$  et  $\mathcal{G} = (y_i)_{i \in I}$  une famille génératrice de  $F$ , ces objets servent ici de notation et seront utilisés indépendamment lors de la preuve.

Montrons que l'image d'une base  $\mathcal{B}$  par une application injective est une famille libre  $\mathcal{F}$ .

Supposons  $f$  injective, donc pour  $(\lambda_i)_{i \in I} \in \mathbb{K}^{(I)}$ ,

$$0_F = \sum_{i \in I} \lambda_i f(e_i) = f\left(\sum_{i \in I} \lambda_i e_i\right) \xrightarrow{f \text{ inj}} \sum_{i \in I} \lambda_i e_i = 0_E \xrightarrow{\mathcal{B} \text{ base donc libre}} (\lambda_i)_{i \in I} = \widetilde{0_{\mathbb{K}}},$$

donc  $f(\mathcal{B}) = \mathcal{F}$  libre.

Supposons qu'il existe  $\mathcal{B}$  telle que  $f(\mathcal{B})$  soit libre, montrons qu'alors  $f$  est injective.

Soit  $x \in \ker f$  :

$$\exists (\lambda_i)_{i \in I} \in \mathbb{K}^{(I)} : 0_F = f(x) = f\left(\sum_{i \in I} \lambda_i e_i\right) = \sum_{i \in I} \lambda_i f(e_i) \xrightarrow{f(\mathcal{B}) \text{ libre}} (\lambda_i)_{i \in I} = \widetilde{0_{\mathbb{K}}},$$

donc  $x = 0_E$  donc  $\ker f = \{0_E\}$  et  $f$  injective.



Montrons que l'image d'une base  $\mathcal{B}$  par une application surjective est une famille génératrice  $\mathcal{G}$ .

Supposons  $f$  surjective. Ainsi,  $\text{Im } f = F$ , or  $\mathcal{B}$  est une base donc est génératrice donc :

$$\text{Vect } f(\mathcal{B}) = f(\text{Vect } \mathcal{B}) = f(E) = \text{Im } f = F,$$

donc  $f(\mathcal{B}) = \mathcal{G}$  est génératrice.

Supposons qu'il existe  $\mathcal{B}$  telle que  $f(\mathcal{B})$  soit génératrice, montrons que  $f$  est surjective.

On a ainsi,

$$F = \text{Vect } f(\mathcal{B}) = f(\text{Vect } \mathcal{B}) = f(E) = \text{Im } f,$$

donc  $f$  surjective.

Montrons que l'image d'une base  $\mathcal{B}$  par un isomorphisme est une base  $\mathcal{B}'$ .

Supposons que  $f$  soit un isomorphisme.  $f$  est injective et  $\mathcal{B}$  est une base donc  $f(\mathcal{B})$  est libre.  $f$  est surjective et  $\mathcal{B}$  est une base donc  $f(\mathcal{B})$  est génératrice. Ainsi,  $f(\mathcal{B}) = \mathcal{B}'$  est une base.

Réciproquement, supposons qu'il existe  $\mathcal{B}$  telle que  $f(\mathcal{B}) = \mathcal{B}'$  soit une base, montrons que  $f$  est un isomorphisme.

$\mathcal{B}'$  est une base donc est libre donc  $f$  est injective.  $\mathcal{B}'$  est une base donc est génératrice donc  $f$  est surjective. Ainsi,  $f$  est un isomorphisme.  $\square$

## 22.6 Caractérisation d'une application linéaire par l'image d'une base

Il existe une unique application linéaire de  $E$  dans  $F$  qui envoie une base donnée de  $E$  sur une famille de  $F$  imposée.

Soient  $(e_i)_{i \in I}$  une base de  $E$  et  $(y_i)_{i \in I}$  une famille de  $F$ .

$$\exists ! f \in \mathcal{L}_{\mathbb{K}}(E, F) : \forall i \in I, f(e_i) = y_i \quad (41)$$

Nous pouvons expliciter une telle application :

$$f \left| \begin{array}{ccc} E & \rightarrow & F \\ \sum_{i \in I} \lambda_i \cdot e_i & \mapsto & \sum_{i \in I} \lambda_i \cdot y_i \end{array} \right. \quad (42)$$

*Démonstration.*

Analyse Supposons qu'il existe  $f \in \mathcal{L}_{\mathbb{K}}(E, F)$  tel que  $\forall i \in I, f(e_i) = y_i$ .

Tout vecteur de  $E$  peut se décomposer de manière unique dans la base  $(e_i)_{i \in I}$ , ce qui détermine son image. Ainsi,  $f$  est unique.

Synthèse Posons une telle application  $f$ .

- $(e_i)_{i \in I}$  est une base donc  $(\lambda_i)_{i \in I}$  est presque nulle et unique donc  $\sum_{i \in I} \lambda_i \cdot y_i$  existe et unique. Ainsi,  $f$  est bien définie.
- Soient  $(\alpha, \beta, x, x') \in \mathbb{K}^2 \times E^2$  fixés quelconques. Notons  $(\lambda_i)_{i \in I}$  et  $(\lambda'_i)_{i \in I}$  les coordonnées de  $x$  et  $x'$  dans  $(e_i)_{i \in I}$ .

$$\begin{aligned} f(\alpha x + \beta x') &= f\left(\alpha \sum_{i \in I} \lambda_i \cdot e_i + \beta \sum_{i \in I} \lambda'_i \cdot e_i\right) \\ &= f\left(\sum_{i \in I} (\alpha \lambda_i + \beta \lambda'_i) \cdot e_i\right) \\ &= \sum_{i \in I} (\alpha \lambda_i + \beta \lambda'_i) \cdot y_i \quad \text{par définition de } f \\ &= \alpha \sum_{i \in I} \lambda_i y_i + \beta \sum_{i \in I} \lambda'_i y_i \\ &= \alpha f(x) + \beta f(x') \end{aligned}$$

Donc  $f$  est linéaire.

— Soit  $j \in I$  fixé quelconque.

$$\begin{aligned} f(e_j) &= f\left(\sum_{i \in I} \delta_{i,j} \cdot e_i\right) \\ &= \sum_{i \in I} \delta_{i,j} \cdot y_i \\ &= y_j \end{aligned}$$

□

## 23 Semaine 23

Pour cette semaine,  $\mathbb{K}$  désigne un corps commutatif,  $E$  et  $F$  des  $\mathbb{K}$ -espaces vectoriels,  $E'$  et  $F'$  des sous-espaces vectoriels respectivement de  $E$  et de  $F$ ,  $I$  un ensemble quelconque non vide.

### 23.1 L'ensemble des automorphisme d'un espace vectoriel muni de la loi de composition forme un groupe

*Démonstration.* Montrons que  $(\mathcal{GL}_{\mathbb{K}}(E), \circ)$  est un sous-groupe de  $(\mathcal{S}(E), \circ)$ .

- $\mathcal{GL}_{\mathbb{K}}(E) \subset \mathcal{S}(E)$  et  $(\mathcal{S}(E), \circ)$  est bien un groupe.
- $\mathcal{GL}_{\mathbb{K}}(E) \neq \emptyset$  puisque  $Id_E \in \mathcal{GL}_{\mathbb{K}}$ .
- Soit  $(f, g) \in \mathcal{GL}(E)$ . Montrons que  $f \circ g^{-1} \in \mathcal{GL}(E)$ .  
Soit  $(\alpha, \beta, x, y) \in \mathbb{K}^2 \times E^2$  fixés quelconques.

$$\begin{aligned}
 (f \circ g^{-1})(\alpha x + \beta y) &= f(g^{-1}(\alpha x + \beta y)) \\
 &= f(g^{-1}(\alpha g^{-1}(g(x)) + \beta g^{-1}(g(y)))) \\
 &= f(g^{-1}(\alpha g(g^{-1}(x)) + \beta g(g^{-1}(y)))) \\
 &= f(g^{-1}(g(\alpha g^{-1}(x) + \beta g^{-1}(y)))) \quad \text{car } g \text{ est linéaire} \\
 &= f(\alpha g^{-1}(x) + \beta g^{-1}(y)) \\
 &= \alpha f(g^{-1}(x)) + \beta f(g^{-1}(y)) \\
 &= \alpha (f \circ g^{-1})(x) + \beta (f \circ g^{-1})(y)
 \end{aligned}$$

□

### 23.2 Caractérisation de la somme directe de $p$ sous-espaces vectoriels

Soit  $(E_i)_{i \in \llbracket 1; p \rrbracket} \subset E^p$   $p$  sous-espace vectoriel de  $E$  avec  $p \in \mathbb{N}^*$  fixé quelconque.

Par définition, cette famille est en somme directe si tout vecteur de  $E_1 + E_2 + \dots + E_p$  peut s'écrire comme une somme unique d'élément de  $E_1 \times E_2 \times \dots \times E_p$ . Formellement :

$$\forall x \in \sum_{i=1}^p E_i, \exists ! x \in \times_{i=1}^p E_i : x = \sum_{i=1}^p x_i \quad (43)$$

Nous allons démontrer que  $E_1, E_2, \dots$  et  $E_p$  sont en somme directe si et seulement si

$$\forall x \in \times_{i=1}^p E_i, \left( \sum_{i=1}^p x_i = 0_E \implies \forall i \in \llbracket 1; p \rrbracket, x_i = 0_E \right) \quad (44)$$

*Démonstration.* Supposons que  $E_1, E_2, \dots, E_p$  sont en somme directe.

Soient  $x \in \times_{i=1}^p E_i$  fixés quelconques tels que  $x_1 + x_2 + \dots + x_p = 0_E$ .

Or  $0_E = \underbrace{0_E}_{\in E_1} + \underbrace{0_E}_{\in E_2} + \dots + \underbrace{0_E}_{\in E_p}$ . Par unicité de l'écriture de  $x$  comme somme d'éléments de  $\times_{i=1}^p E_i$ ,

$\forall i \in \llbracket 1; p \rrbracket, x_i = 0_E$ .

Supposons maintenant l'équation de la caractérisation.

Soit  $x \in \times_{i=1}^p E_i$  tel que  $x$  puisse s'écrire comme somme de  $x' \in \times_{i=1}^p E_i$  et somme de  $x'' \in \times_{i=1}^p E_i$ . Montrons que  $x' = x''$ .

$$\sum_{i=1}^p x'_i = x = \sum_{i=1}^p x''_i$$

Donc

$$\sum_{i=1}^p (x'_i - x''_i) = 0_E$$

D'après l'équation de la caractérisation,  $\forall i \in \llbracket 1; p \rrbracket, x'_i - x''_i = 0_E$ .

Donc  $\forall i \in \llbracket 1; p \rrbracket, x'_i = x''_i$

□

## 24 Semaine 24

Pour cette semaine,  $\mathbb{K}$  désigne un corps commutatif,  $E$  et  $F$  des  $\mathbb{K}$ -espaces vectoriels,  $E'$  et  $F'$  des sous-espaces vectoriels respectivement de  $E$  et de  $F$ .

Nous rappelons que  $\dim\{0_E\} = 0$  et que  $\{0_E\} = \text{Vect } \emptyset$ .

### 24.1 Existence d'un supplémentaire en dimension finie

Pour tout sous-espace vectoriel de  $E$ , il existe un sous-espace vectoriel complémentaire.

*Démonstration.*

*Théorème de la base incomplète* (admis ici mais démontré dans le cours) : pour toute famille libre de  $E$ , nous pouvons y adjoindre une partie d'une famille quelconque génératrice de  $E$  (généralement une base, la base canonique si elle a un sens) pour en faire une base de  $E$ .

Posons  $n = \dim E$  et  $p = \dim E'$ . Ainsi, il existe  $(e_1, \dots, e_p)$  base de  $E'$ . Appliquons le théorème de la base incomplète pour cette famille. Il existe  $(e_{p+1}, \dots, e_n)$   $n - p$  vecteurs de  $E$  tel que  $(e_1, \dots, e_n)$  est une base de  $E$ . Posons  $E'' = \text{Vect } \{e_{p+1}, \dots, e_n\}$  et vérifions qu'il est supplémentaire à  $E'$ .

Par définition de  $\text{Vect}$ ,  $E''$  est un sous-espace vectoriel. Trivialement,  $E' + E'' = E$ .  $\{0_E\} \subset E' \cap E''$  car  $E'$  et  $E''$  sont deux sous-espaces vectoriels. Soit  $x \in E' \cap E''$ .  $x \in E' \implies \exists (\lambda_1, \dots, \lambda_p) \in \mathbb{K}^p : x = \sum_{i=1}^p \lambda_i e_i$  et  $x \in E'' \implies \exists (\lambda_{p+1}, \dots, \lambda_n) \in \mathbb{K}^{n-p} : x = \sum_{i=p+1}^n \lambda_i e_i$ . Par différence,  $\sum_{i=1}^p \lambda_i e_i + \sum_{i=p+1}^n (-\lambda_i) e_i = 0_E$ . Or  $(e_i)_{i \in \llbracket 1; n \rrbracket}$  est une base de  $E$  donc  $\forall i \in \llbracket 1; p \rrbracket, \lambda_i = 0_{\mathbb{K}}$ . donc  $x = 0_E$ . Ainsi,  $E' \cap E'' = \{0_E\}$ .  $\square$

### 24.2 Dimension de $\mathcal{L}_{\mathbb{K}}(E, F)$

$\mathcal{L}_{\mathbb{K}}(E, F)$  est dimension finie et

$$\dim \mathcal{L}_{\mathbb{K}}(E, F) = \dim E \times \dim F \quad (45)$$

*Démonstration.* Notons  $n = \dim E$  et  $(e_i)_{i \in \llbracket 1; n \rrbracket}$  une base de  $E$ . Considérons

$$\varphi \left| \begin{array}{ccc} \mathcal{L}_{\mathbb{K}}(E, F) & \rightarrow & F^n \\ f & \mapsto & (f(e_i))_{i \in \llbracket 1; n \rrbracket} \end{array} \right.$$

$\varphi$  est linéaire et, d'après le théorème de création des applications linéaires, bijective. Ainsi,  $\mathcal{L}_{\mathbb{K}}(E, F)$  et  $F^n$  sont isomorphes.  $F^n$  est de dimension finie, ce qui conclut.  $\square$

### 24.3 Formule de Grassman

Supposons  $E$  de dimension finie.

Soient  $E_1$  et  $E_2$  deux sous-espaces vectoriels. Alors  $E_1 + E_2$  est de dimension finie et

$$\dim E_1 + E_2 = \dim E_1 + \dim E_2 - \dim E_1 \cap E_2 \quad (46)$$

*Démonstration.* Commençons par prouver une version simplifiée de la somme directe. Supposons que  $E_1$  et  $E_2$  sont en somme directe.

Fixons  $\mathcal{B}_1$  et  $\mathcal{B}_2$  deux bases de  $E_1$  et  $E_2$ . Alors  $(\mathcal{B}_1, \mathcal{B}_2)$  engendre  $E_1 + E_2$ . Or  $(\mathcal{B}_1, \mathcal{B}_2)$  est finie donc  $E_1 + E_2$  est de dimension finie.

Posons  $n = \dim E_1$  et  $p = \dim E_2$ . Notons  $(e_i)_{i \in \llbracket 1; n \rrbracket}$  la base  $\mathcal{B}_1$  et  $(f_i)_{i \in \llbracket 1; p \rrbracket}$  la base  $\mathcal{B}_2$ .

Soient  $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_p \in \mathbb{K}^{n+p}$  fixés quelconques tels que  $\sum_{i=1}^n \lambda_i e_i + \sum_{i=1}^p \mu_i f_i = 0_E$ . Alors  $\sum_{i=1}^n \lambda_i e_i = \sum_{i=1}^p (-\mu_i) f_i$ . Or  $\sum_{i=1}^n \lambda_i e_i \in E_1$  et  $\sum_{i=1}^p (-\mu_i) f_i \in E_2$  donc  $\sum_{i=1}^n \lambda_i e_i \in E_1 \cap E_2 = \{0_E\}$ . Donc  $\lambda = \tilde{0}$ . De même,  $\mu = \tilde{0}$ . Donc  $(\mathcal{B}_1, \mathcal{B}_2)$  est libre.

Ainsi,  $(\mathcal{B}_1, \mathcal{B}_2)$  est une base de  $E_1 \oplus E_2$ . Donc  $\dim E_1 \oplus E_2 = |(\mathcal{B}_1, \mathcal{B}_2)| = |\mathcal{B}_1| + |\mathcal{B}_2| = \dim E_1 + \dim E_2$ .

Enlevons l'hypothèse que  $E_1$  et  $E_2$  sont en somme directe.  $E_1 \cap E_2$  est un sous-espace vectoriel de  $E_2$ . Comme  $E_2$  est un  $\mathbb{K}$ -espace vectoriel de dimension finie, il existe  $E'_2$  sous-espace vectoriel de  $E_2$  tel que  $E_2 = (E_1 \cap E_2) \oplus E'_2$ .

Montrons que  $E_1 + E_2 = E_1 \oplus E'_2$ .

$$\begin{aligned} E_1 \cap E'_2 &= E_1 \cap (E'_2 \cap E_2) \text{ car } E'_2 \subset E_2 \\ &= (E_1 \cap E_2) \cap E'_2 \text{ car } \cap \text{ est associative et commutative} \\ &= 0_E \text{ car } E_1 \text{ et } E_2 \text{ sont en somme directe et } E'_2 \text{ sev} \end{aligned}$$

Donc  $E_1$  et  $E'_2$  sont en somme directe.

$E'_2 \subset E_2$  donc  $E_1 + E'_2 \subset E_1 + E_2$ . Soit  $x \in E_1 + E_2$ . Alors  $\exists (x_1, x_2) \in E_1 \times E_2 : x = x_1 + x_2$ . Or  $E_2 = (E_1 \cap E_2) \oplus E'_2$  donc  $\exists (x_{21}, x'_2) \in E_1 \times E'_2 : x_2 = x_{21} + x'_2$ . D'où  $x = x_1 + x_{21} + x'_2$ . Or  $x_1 + x_{21} \in E_1$  et  $x'_2 \in E'_2$  donc  $x \in E_1 + E'_2$ .

Ainsi,  $E_1$  et  $E'_2$  étant des sous-espace vectoriel de dimension finie,  $\dim E_1 \oplus E'_2 = \dim E_1 + \dim E'_2$ . De plus,  $\dim E_2 = \dim(E_1 \cap E_2) \oplus E'_2 = \dim E_1 \cap E_2 + \dim E'_2$ . Donc  $\dim E_1 + E_2 = \dim E_1 + \dim E_2 - \dim E_1 \cap E_2$ .  $\square$

## 24.4 Caractérisation injectivité/bijektivité/surjectivité par le rang

Soit  $f \in \mathcal{L}_{\mathbb{K}}(E, F)$ .

(i) Si  $E$  est de dimension finie

$$f \text{ injective} \iff \text{rg} f = \dim E \quad (47)$$

(ii) Si  $F$  est de dimension finie

$$f \text{ surjective} \iff \text{rg} f = \dim F \quad (48)$$

(iii) Si  $E$  et  $F$  sont de même dimension finie

$$f \text{ bijective} \iff f \text{ injective} \iff f \text{ surjective}$$

C'est l'accident de la dimension finie !

*Démonstration.*

(i) Supposons  $E$  de dimension finie, fixons  $(e_1, \dots, e_n)$  une base de  $E$  (avec  $n = \dim E$ ) Supposons  $f$  injective :

$$\text{rg} f = \dim \text{Im} f = \dim \text{Vect} \{f(e_1) \dots f(e_n)\}$$

Donc  $(f(e_1), \dots, f(e_n))$  est génératrice.  $(f(e_1), \dots, f(e_n))$  est de plus libre car  $f$  est injective. Donc c'est une base, donc

$$\dim \text{Vect} \{f(e_1) \dots f(e_n)\} = n = \dim E$$

donc  $\text{rg} f = \dim E$ . Réciproquement, supposons que  $\text{rg} f = \dim E = n$ . Alors

$$n = \text{rg} f = \dim \text{Vect} \{f(e_1), \dots, f(e_n)\}$$

Donc  $(f(e_1), \dots, f(e_n))$  est génératrice de cardinal  $n$ , égal à la dimension du sous-espace vectoriel engendré. C'est donc une base du sous-espace vectoriel engendré. Donc  $(f(e_1), \dots, f(e_n))$  est libre, donc  $f$  est injective.

(ii) Supposons  $F$  de dimension finie

$$f \text{ surjective} \iff \text{Im} f = F \iff \dim \text{Im} f = \dim F$$

(iii) Supposons  $E$  et  $F$  de même dimension finie

$$f \text{ injective} \iff \text{rg} f = \dim E \iff \text{rg} f = \dim F \iff f \text{ surjective}$$

D'où la bijectivité.  $\square$

## 24.5 Théorème du rang

Si  $E$  est de dimension finie alors pour toute  $f \in \mathcal{L}_{\mathbb{K}}(E, F)$  application linéaire,

$$\dim E = \text{rg } f + \dim \ker f \quad (49)$$

*Démonstration.* Démontrons d'abord le lemme suivant. Soient  $f \in \mathcal{L}_{\mathbb{K}}(E, F)$  et  $H$  un supplémentaire de  $\ker f$  dans  $E$ . Alors  $f|_H^{\text{Im} f}$  est un isomorphisme de  $H$  sur  $\text{Im} f$ .

Notons  $\hat{f}$  une telle restriction et corestriction. Cette application est bien définie (car  $f(H) \subset \text{Im} f$ ) et  $\hat{f} \in \mathcal{L}_{\mathbb{K}}(H, \text{Im} f)$ .

Calculons son noyau.  $\ker \hat{f} = \{x \in H \mid \hat{f}(x) = 0_E\} = \{x \in H \mid x \in \ker f\} = H \cap \ker f = \{0_E\}$  car  $H$  et  $\ker f$  sont complémentaires. Donc  $\hat{f}$  est injective.

Soit  $y \in \text{Im} f$ . D'où  $\exists x \in E : y = f(x)$ . Décomposons  $x$  dans  $E = H \oplus \ker f$ ,  $\exists (x_H, x_k) \in H \times \ker f : x = x_H + x_k$ . Ainsi,  $y = f(x) = f(x_H) + f(x_k) = f(x_H)$  car  $x_k \in \ker f$ . Donc  $y$  admet un antécédent par  $\hat{f}$  (qui est  $x_H$ ). Donc  $\hat{f}$  est surjective.

Donc  $f|_H^{\text{Im} f}$  est un isomorphisme de  $H$  sur  $\text{Im} f$ .

Supposons maintenant que  $E$  est de dimension finie. Soit  $f \in \mathcal{L}_{\mathbb{K}}(E, F)$ . D'après le théorème d'existence d'un supplémentaire en dimension finie,  $\ker f$ , étant un sous-espace vectoriel de  $E$ , admet un supplémentaire  $H$  c'est-à-dire  $E = H \oplus \ker f$ . En prenant la dimension sur cette égalité,  $\dim E = \dim \ker f + \dim H$ . D'après le lemme précédent,  $\dim H = \dim \text{Im} f = \text{rg } f$ . D'où  $\dim E = \text{rg } f + \dim \ker f$ .  $\square$

## 24.6 Rang d'une composition d'applications linéaires

Soit  $G$  un  $\mathbb{K}$ -espace vectoriel et  $(u, v) \in \mathcal{L}_{\mathbb{K}}(E, F) \times \mathcal{L}_{\mathbb{K}}(F, G)$ . Si  $E$  et  $F$  sont de dimension finie alors

$$\text{rg } u = \text{rg } v \circ u + \dim \ker v \cap \text{Im } u \quad (50)$$

*Démonstration.* Considérons que  $E$  et  $F$  sont de dimension finie. Soient de tels objets. Appliquons le théorème du rang à  $v|_{\text{Im } u}$  ce qui est autorisé puisque  $v|_{\text{Im } u}$  est une application linéaire et  $\text{Im } u$  est un  $\mathbb{K}$ -espace vectoriel de dimension finie (car sev de  $F$ ).

$$\dim \text{Im } u = \text{rg } v|_{\text{Im } u} + \dim \ker v|_{\text{Im } u}$$

Ainsi,  $\ker v|_{\text{Im } u} = \{y \in \text{Im } u \mid v(y) = 0_G\} = \{y \in \text{Im } u \mid y \in \ker v\} = \text{Im } u \cap \ker v$  et  $\text{Im } v|_{\text{Im } u} = v(\text{Im } u) = \text{Im } v \circ u$  (cette égalité est vraie pour deux fonctions de  $E$  dans  $F$  et de  $F$  dans  $G$  quelconques, pas forcément linéaires). Ce qui conclut.  $\square$

## 24.7 Caractérisation des hyperplans

Soit  $H$  un sous-espace vectoriel de  $E$ . Les conditions suivantes sont équivalentes :

- (i)  $H$  est un hyperplan de  $E : \exists \varphi \in E^* : H = \ker \varphi$
- (ii)  $H$  admet une droite vectorielle comme supplémentaire :  $\exists a \in E \setminus \{0_E\} : H \oplus \text{Vect } \{a\} = E$

*Démonstration.* (i)  $\implies$  (ii) Supposons que  $H$  est un hyperplan de  $E$ . Appliquons la définition de l'hyperplan,  $\exists \varphi \in E^* : H = \ker \varphi$ . Par l'absurde, supposons que  $E \setminus H = \emptyset$ . Or  $H \subset E$  donc  $E = H$ . Donc  $\varphi = 0_{E^*}$  ce qui est une contradiction.

Ainsi fixons  $a \in E \setminus H$  quelconque. Montrons que  $E = H \oplus \text{Vect } \{a\}$ . Trivialement,  $\{0_E\} \subset H \cap \text{Vect } \{a\}$ . Soit  $x \in H \cap \text{Vect } \{a\}$ .  $x \in \text{Vect } \{a\}$  donc  $\exists \lambda \in \mathbb{K} : x = \lambda a$ . De plus,  $x \in H = \ker \varphi$  donc  $0_{\mathbb{K}} = \varphi(x) = \lambda \varphi(a)$ . Si  $\lambda \neq 0_{\mathbb{K}}$ , alors  $a \in \ker \varphi$  ce qui est impossible car  $a \notin H$ . Donc  $\lambda = 0_{\mathbb{K}}$ , d'où  $x = 0_E$ . Ainsi,  $H \cap \text{Vect } \{a\} = \{0_E\}$ .  $H$  et  $\text{Vect } \{a\}$  sont en somme directe.

Trivialement,  $H + \text{Vect } \{a\} \subset E$ . Soit  $x \in E$  fixé quelconque.  $a \notin H$  donc  $\varphi(a) \neq 0_{\mathbb{K}}$ .  $\varphi(a)$  est inversible dans  $\mathbb{K}$  d'où :

$$\varphi(x) = \frac{\varphi(x)}{\varphi(a)} \cdot \varphi(a) = \varphi\left(\frac{\varphi(x)}{\varphi(a)} \times a\right)$$

Donc  $x - \frac{\varphi(x)}{\varphi(a)} \cdot a \in H$ . D'où

$$x = \underbrace{x - \frac{\varphi(x)}{\varphi(a)} \cdot a}_{\in H} + \underbrace{\frac{\varphi(x)}{\varphi(a)} \cdot a}_{\in \text{Vect } \{a\}}$$

Ainsi,  $E = H + \text{Vect } \{a\}$ .

(ii)  $\implies$  (i) Supposons maintenant que  $H$  soit un sous-espace vectoriel tel que  $\exists a \in E \setminus \{0_E\} : E = H \oplus \text{Vect } \{a\}$ . Posons  $\varphi : \begin{matrix} E &= & H \oplus \text{Vect } \{a\} &\rightarrow & \mathbb{K} \\ x &= & h_x + \lambda_x \cdot a &\mapsto & \lambda_x \end{matrix}$ . Montrons que  $\varphi$  est une forme linéaire non triviale dont  $H$  est le noyau.

$\varphi$  est bien définie (car  $h_x$  et  $\lambda_x$  sont uniques), linéaire, à valeur dans le corps de base  $\mathbb{K}$  donc  $\varphi$  est une forme linéaire.  $\varphi \neq 0_{E^*}$  car  $\varphi(a) = 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ . Soit  $x \in E$  fixé quelconque. Alors  $\exists (h_x, \lambda_x) \in H \times \mathbb{K} : x = h_x + \lambda_x \cdot a$ .

$$x \in \ker \varphi \iff \varphi(x) = 0_{\mathbb{K}} \iff \lambda_x = 0_{\mathbb{K}} \iff x \in H$$

donc  $\ker \varphi = H$ . Donc  $H$  est un hyperplan de  $E$ .

Si  $E$  est de dimension finie, alors les deux conditions sont équivalentes à

(iii)  $H$  est de codimension 1 c'est-à-dire de dimension  $n - 1$ .

(ii)  $\implies$  (iii) Il faut prendre la dimension de l'égalité  $H \oplus \text{Vect } \{a\}$ .

(iii)  $\implies$  (ii) Supposons que  $\dim H = n - 1$ . Comme  $E$  est de dimension finie,  $H$  admet un supplémentaire  $I$  dans  $E : H \oplus I = E$ . En prenant la dimension,  $\dim I = 1$ . Donc  $I$  est une droite vectorielle. D'où  $\exists a \in E : I = \text{Vect } \{a\}$ .  $a \notin H$  car sinon  $I \subset H$  ce qui contredit  $I \cap H = \{0_E\}$  ( $I$  et  $H$  sont en somme directe).  $\square$

## 24.8 Proportionnalité des formes linéaires ayant le même noyau

*Lemme fondamental dans l'étude des formes linéaires* Soit  $\varphi \in E^* \setminus \{0_{E^*}\}$ .

Tout vecteur de  $E$  n'appartenant pas au noyau de  $\varphi$  engendre une droite qui est supplémentaire au noyau de  $\varphi$  dans  $E$ .

$$\forall a \in E \setminus \ker \varphi, E = \ker \varphi \oplus \text{Vect } \{a\} \quad (51)$$

Deux formes linéaires non nulles  $\varphi$  et  $\psi$  ont le même noyau si et seulement si elles sont proportionnelles ce qui revient à dire que la famille  $(\varphi, \psi)$  est liée.

$$\forall (\varphi, \psi) \in (E^* \setminus \{0_{E^*}\})^2, \ker \varphi = \ker \psi \iff \exists \lambda \in \mathbb{K}^* : \varphi = \lambda \cdot \psi \quad (52)$$

*Démonstration.* Commençons par prouver le lemme. Soit  $a \in E \setminus \ker \varphi$ .

Soit  $x \in E$  fixé quelconque. Exhibons la décomposition unique de  $x$  dans  $\ker \varphi + \text{Vect } \{a\}$ .

*Analyse* Supposons qu'il existe  $(x_k, \lambda) \in \ker \varphi \times \mathbb{K}$  tel que  $x = x_k + \lambda a$ . Puisque  $x_k \in \ker \varphi$ ,  $\varphi(x) = \lambda \cdot \varphi(a)$ . Or  $\varphi(a) \neq 0_{\mathbb{K}}$  (car  $a \notin \ker \varphi$ ) donc  $\varphi(a)$  est inversible dans  $\mathbb{K}$ . D'où  $\lambda = \varphi(x)/\varphi(a)$  et  $x_k = x - \varphi(x)/\varphi(a) \cdot a$ .

Ainsi, sous réserve d'existence,  $\lambda$  et  $x_k$  sont uniques.

*Synthèse* Posons  $\begin{cases} \lambda &= & \frac{\varphi(x)}{\varphi(a)} \\ x_k &= & x - \frac{\varphi(x)}{\varphi(a)} a \end{cases}$  Nous avons bien  $x = x_k + \lambda \cdot a$ ,  $\lambda \cdot a \in \text{Vect } \{a\}$  (car  $\lambda \in \mathbb{K}$ )

et  $x_k \in \ker \varphi$  (car  $\varphi(x_k) = \varphi(x) - \varphi\left(\frac{\varphi(x)}{\varphi(a)} a\right) = \varphi(x) - \frac{\varphi(x)}{\varphi(a)} \varphi(a) = 0_{\mathbb{K}}$ ). Ainsi  $E = \ker \varphi \oplus \text{Vect } \{a\}$ .

Soient  $(\varphi, \psi) \in (E^* \setminus \{0_{E^*}\})^2$  fixés quelconques.

*Sens direct* Supposons que  $\ker \varphi = \ker \psi$ .  $\varphi \neq 0_{E^*}$  donc  $\ker \varphi \neq E$  donc  $\exists a \in E : a \notin \ker \varphi$ . Appliquons la lemme ci-dessus :

$$\begin{aligned} E &= \begin{matrix} \ker \varphi \\ \parallel \\ \ker \psi \end{matrix} \oplus \text{Vect } \{a\} \rightarrow \mathbb{K} \\ \varphi : x &= \left( x - \frac{\varphi(x)}{\varphi(a)} \cdot a \right) + \frac{\varphi(x)}{\varphi(a)} \cdot a \mapsto \varphi(x) \\ \psi : x &= \left( x - \frac{\varphi(x)}{\varphi(a)} \cdot a \right) + \frac{\varphi(x)}{\varphi(a)} \cdot a \mapsto \psi(x) \end{aligned}$$

Or  $\left( x - \frac{\varphi(x)}{\varphi(a)} \cdot a \right) \in \ker \psi$  donc  $\psi(x) = \frac{\psi(a)}{\varphi(a)} \varphi(x)$ . Ainsi,  $\psi = \frac{\psi(a)}{\varphi(a)} \varphi$ . Donc  $\varphi$  et  $\psi$  sont proportionnelles.

*Sens réciproque* Supposons que  $\varphi$  et  $\psi$  sont proportionnelles. Alors  $\exists \lambda \in \mathbb{K}^* : \varphi = \lambda \psi$ .  $\varphi = \lambda \psi \implies \ker \psi \subset \ker \varphi$  et  $\psi = \lambda^{-1} \varphi \implies \ker \varphi \subset \ker \psi$ . Ce qui donne l'égalité.  $\square$

## 24.9 Intersection d'hyperplans

Soit  $\varphi \in E^*$  une forme linéaire *non nulle*. Soit  $F$  un sous-espace vectoriel de  $E$  de dimension finie  $p \in \mathbb{N}$ , alors

$$\dim_{\mathbb{K}} F \cap \ker \varphi = \begin{cases} p & \text{si } F \subset \ker \varphi \\ p-1 & \text{sinon} \end{cases} \quad (53)$$

En particulier, on a toujours  $\dim_{\mathbb{K}} F \cap \ker \varphi \geq p-1$

Supposons que  $E$  un  $\mathbb{K}$ -espace vectoriel de dimension finie  $n \in \mathbb{N}^*$ . Soient  $m \in \mathbb{N}^*$  et  $(H_i)_{i \in [1, m]}$ ,  $m$  hyperplans de  $E$ . Alors

$$\dim_{\mathbb{K}} \bigcap_{i=1}^m H_i \geq n - m \quad (54)$$

*Démonstration.* Si  $F \subset \ker \varphi$ ,  $F \cap \ker \varphi = F$  donc  $\dim F \cap \ker \varphi = p$

Sinon, il existe  $a \in F$  tel que  $a \notin \ker \varphi$ . Ainsi,

$$\text{Vect}\{a\} \oplus \ker \varphi = E$$

Montrons alors que  $F = \text{Vect}\{a\} \oplus (F \cap \ker \varphi)$ .

$$\text{Vect}\{a\} \cap (F \cap \ker \varphi) = \underbrace{\text{Vect}\{a\} \cap F \cap \ker \varphi}_{=\text{Vect}\{a\}} = \text{Vect}\{a\} \cap \ker \varphi = \{0_E\}$$

car les deux espaces sont supplémentaires donc en somme directe.

Par double inclusion, montrons que  $\text{Vect}\{a\} + (F \cap \ker \varphi) = F$ . Pour l'inclusion directe, remarquons que  $a \in F$  donc  $\text{Vect}\{a\} \subset F$  or  $F \cap \ker \varphi \subset F$  donc leur somme est bien incluse  $\text{Vect}\{a\} + (F \cap \ker \varphi) \subset F$ . Réciproquement, soit  $x \in F$  fixé quelconque. Puisque  $\text{Vect}\{a\} \oplus \ker \varphi = E$

$$\exists (\lambda, x_K) \in \mathbb{K} \times \ker \varphi : x = \lambda.a + x_K$$

De plus,  $x_K = x - \lambda.a \in F$  car  $(a, x) \in F^2$  donc

$$x = \underbrace{\lambda.a}_{\in \text{Vect}\{a\}} + \underbrace{x_K}_{\in F \cap \ker \varphi} \in \text{Vect}\{a\} + (F \cap \ker \varphi)$$

D'où l'inclusion réciproque.

Donc  $F = \text{Vect}\{a\} \oplus (F \cap \ker \varphi)$ . En passant à la dimension :

$$\underbrace{\dim F}_{=p} = \underbrace{\dim \text{Vect}\{a\}}_{=1} + \dim(F \cap \ker \varphi)$$

Donc  $\dim(F \cap \ker \varphi) = p - 1$ .

Considérons la propriété  $\mathcal{P}(\cdot)$  définie pour tout  $m \in \mathbb{N}^*$  par :

$$\mathcal{P}(m) : \text{“ pour tous } H_1, \dots, H_m \text{ hyperplans de } E, \dim_{\mathbb{K}} \bigcap_{i=1}^m H_i \geq n - m \text{”}$$

Soit  $H_1$  un hyperplan de  $E$  fixé quelconque. D'après la caractérisation des hyperplans en dimension finie,

$$\dim_{\mathbb{K}} \bigcap_{i=1}^1 H_i = \dim_{\mathbb{K}} H_1 = n - 1 \geq n - 1$$

Donc  $\mathcal{P}(1)$  est vraie.

Soit  $m \in \mathbb{N}^*$  fixé quelconque tel que  $\mathcal{P}(m)$  est vraie. Soient  $H_1, \dots, H_m$  et  $H_{m+1}$   $m+1$  hyperplans de  $E$ . D'après la définition d'un hyperplan, il existe  $\varphi \in E^*$  non nulle telle que  $H_{m+1} = \ker \varphi$ .

Appliquons donc le lemme précédent pour  $F \leftarrow \bigcap_{i=1}^m H_i$  (autorisé car c'est un sous espace de l'espace  $E$ , qui est de dimension finie, donc ses sous espaces les sont aussi) et  $\varphi \leftarrow \varphi$  (autorisé car c'est une forme linéaire non nulle) :



$$\dim_{\mathbb{K}} \underbrace{\left( \bigcap_{i=1}^m H_i \right) \cap \ker \varphi}_{= (\bigcap_{i=1}^m H_i) \cap H_{m+1}} \geq \dim_{\mathbb{K}} \left( \bigcap_{i=1}^m H_i \right) - 1 \quad \underbrace{\geq n - m - 1}_{\text{en appliquant } \mathcal{P}(m) \text{ pour } H_1, \dots, H_m}$$

Donc par associativité de l'intersection,  $\dim_{\mathbb{K}} \bigcap_{i=1}^{m+1} H_i \geq n - (m + 1)$ . Donc  $\mathcal{P}(m + 1)$  est vraie.  $\square$

## 25 Semaine 25

### 25.1 S'il existe un inverse à droite (ou à gauche) pour une matrice carrée, alors celle ci est inversible

Soit  $A \in \mathcal{M}_n(\mathbb{K})$

- S'il existe  $B \in \mathcal{M}_n(\mathbb{K}) : A \times B = I_n$ , alors  $A \in GL_n(\mathbb{K})$  et  $A^{-1} = B$
- S'il existe  $B \in \mathcal{M}_n(\mathbb{K}) : B \times A = I_n$ , alors  $A \in GL_n(\mathbb{K})$  et  $A^{-1} = B$

*Démonstration.* Supposons  $\exists B \in \mathcal{M}_n(\mathbb{K}) : A \times B = I_n$ . Notons  $(\hat{a}, \hat{b}) \in \mathcal{L}(\mathbb{K}^n)$  les endomorphismes canoniquement associés à  $A$  et à  $B$ .

$$\begin{aligned}
 \Phi_{\mathcal{B}_{\text{can } \mathbb{K}^n}}(\hat{a} \circ \hat{b}) &= \text{mat}(\hat{a} \circ \hat{b}, \mathcal{B}_{\text{can } \mathbb{K}^n}, \mathcal{B}_{\text{can } \mathbb{K}^n}) \\
 &= \text{mat}(\hat{a}, \mathcal{B}_{\text{can } \mathbb{K}^n}, \mathcal{B}_{\text{can } \mathbb{K}^n}) \times_{\mathcal{M}_\setminus(\mathbb{K})} \text{mat}(\hat{b}, \mathcal{B}_{\text{can } \mathbb{K}^n}, \mathcal{B}_{\text{can } \mathbb{K}^n}) \\
 &= A \times B \\
 &= I_n \\
 &= \text{mat}(\text{Id}_{\mathbb{K}^n}, \mathcal{B}_{\text{can } \mathbb{K}^n}, \mathcal{B}_{\text{can } \mathbb{K}^n}) = \Phi_{\mathcal{B}_{\text{can } \mathbb{K}^n}}(\text{Id}_{\mathbb{K}^n})
 \end{aligned}$$

D'où, par injectivité de  $\Phi_{\mathcal{B}_{\text{can } \mathbb{K}^n}}$ ,  $\hat{a} \circ \hat{b} = \text{Id}_{\mathbb{K}^n}$ .

Ainsi,  $\hat{a} \circ \hat{b}$  est surjective, donc  $\hat{a}$  est surjective, mais par l'accident de la dimension finie,  $\hat{a}$  est bijective, donc c'est un automorphisme, donc toutes ses matrices associées sont inversibles. On effectue un même raisonnement pour l'inversibilité à gauche, en utilisant cette fois l'injectivité.  $\square$

## **26    Semaine 26**

Cette semaine avais trois jours fériés : les khôlles furent annulées.

## 27 Semaine 27

### 27.1 Norme uniforme d'une fonction continue par morceaux

Soit  $f \in \mathcal{CM}([a; b], \mathbb{R})$ .

L'ensemble  $\{|f(t)| \mid t \in [a; b]\}$  admet une borne supérieure notée  $\|f\|_{\infty, [a; b]}$ .

*Démonstration.* Montrons que sur chaque morceau,  $f$  est bornée.

Soit  $\sigma = (x_i)_{0 \leq i \leq N} \in \mathcal{S}([a; b])$  adaptée à  $f$ . Soit  $i \in \llbracket 0; N-1 \rrbracket$ . Posons  $f_i = f|_{[x_i; x_{i+1}[}$ .  $f$  étant continue par morceaux,  $\exists (l_i^+, l_{i+1}^-) \in \mathbb{R}^2 : \lim_{x \rightarrow x_i^+} f_i(x) = l_i^+ \wedge \lim_{x \rightarrow x_{i+1}^-} f_i(x) = l_{i+1}^-$ . Nous pouvons

donc prolonger  $f_i$  en  $\tilde{f}_i$  par continuité en  $x_i$  et en  $x_{i+1}$ . Comme  $f \in \mathcal{C}^0([a; b], \mathbb{R})$ , le théorème de Weierstrass s'applique :  $\text{Im } \tilde{f}_i$  est bornée (donc  $f_i$  aussi). Ainsi  $\|f_i\|_{\infty, [a; b]}$  est bien défini.

$\{|f(t)| \mid t \in [a; b]\}$  est :

- une partie de  $\mathbb{R}$
- non vide car contenant  $|f(x)|$ .
- majorée par  $\max \left( \{\|f_i\|_{\infty, [a; b]} \mid i \in \llbracket 0; N-1 \rrbracket\} \cup \{\|f_i\|_{\infty, [a; b]} \mid i \in \llbracket 0; N-1 \rrbracket\} \right)$  (ensemble admettant bien un plus grand élément puisque fini)

Donc  $\|f\|_{\infty, [a; b]}$  est bien définie.

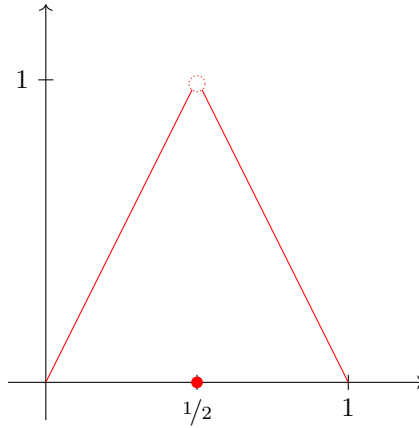


FIGURE 4 –  $\|f\|_{\infty, [a; b]}$  peut ne pas être atteinte

□

### 27.2 Lemme d'approximation uniforme d'une fonction continue sur un segment par une fonction en escalier

Soit  $f \in \mathcal{C}^0([a; b], \mathbb{R})$ .

- (i)  $\forall \varepsilon \in \mathbb{R}_+^*, \exists \chi \in \mathcal{E}([a; b], \mathbb{R}) : \|f - \chi\|_{\infty, [a; b]} \leq \varepsilon$
- (ii)  $\forall \varepsilon \in \mathbb{R}_+^*, \exists (\varphi, \psi) \in \mathcal{E}([a; b], \mathbb{R})^2 : \begin{cases} \varphi \leq f \leq \psi \\ \|\psi - \varphi\|_{\infty, [a; b]} \leq \varepsilon \end{cases}$

*Démonstration.* Soit  $f \in \mathcal{C}^0([a; b], \mathbb{R})$ . Soit  $\varepsilon \in \mathbb{R}_+^*$  fixé quelconque.

(i) D'après le théorème de Heine,  $f \in \mathcal{C}_u^0([a; b], \mathbb{R})$ . Écrivons la définition de uniformément continue pour  $\varepsilon$  :

$$\exists \eta \in \mathbb{R}_+^* : \forall (x, y) \in [a; b]^2, |x - y| \leq \eta \implies |f(x) - f(y)| \leq \varepsilon$$

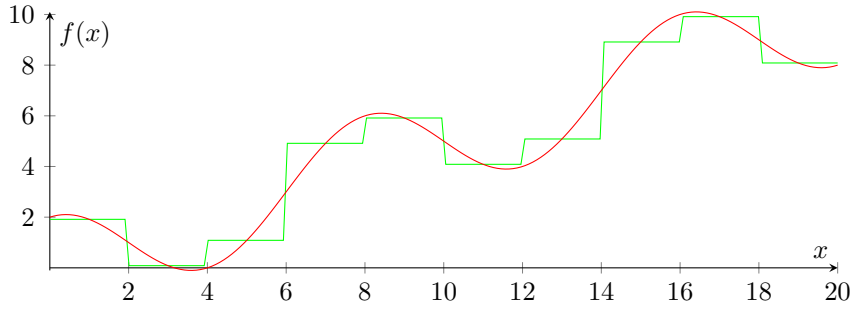


FIGURE 5 – Fonction en escalier "approximant" une fonction continue

Cherchons  $N$  tel que  $\frac{b-a}{N} \leq 2\eta$ . C'est-à-dire  $N \geq \frac{b-a}{2\eta}$ . Posons donc  $N = \lceil \frac{b-a}{2\eta} \rceil$  et  $\eta' = \frac{b-a}{N}$  de sorte que  $\eta' \leq 2\eta$ .

Définissons  $\chi \in \mathcal{E}([a; b], \mathbb{R})$  par

$$\chi \left| \begin{array}{ll} [a; b] & \rightarrow \mathbb{R} \\ x & \mapsto \begin{cases} f(x) & \text{si } \exists n \in \mathbb{N} : x = a + n\eta' \\ f\left(a + \eta' \left(\lfloor \frac{x-a}{\eta'} \rfloor + 1/2\right)\right) & \text{sinon} \end{cases} \end{array} \right.$$

Ceci est bien une fonction en escalier car  $(a + k\eta')_{0 \leq k \leq N}$  est une subdivision adaptée. En effet,  $\forall k \in \llbracket 0; N-1 \rrbracket$ ,  $f|_{[a+k\eta'; a+(k+1)\eta']} = f\left(a + \eta' \left(\lfloor \frac{x-a}{\eta'} \rfloor + 1/2\right)\right) \cdot \tilde{1}_{[a+k\eta'; a+(k+1)\eta']}$ .

Soit  $x \in [a; b]$ . Si  $\exists n \in \mathbb{N} : x = a + n\eta'$  alors  $|f(x) - \chi(x)| = 0$ . Sinon  $0 \leq \frac{x-a}{\eta'} - \lfloor \frac{x-a}{\eta'} \rfloor \leq 1$ . D'où  $0 \leq (x-a) - \eta' \lfloor \frac{x-a}{\eta'} \rfloor \leq \eta'$ . Donc, en enlevant  $\eta'/2$ ,  $-\frac{\eta'}{2} \leq a + \eta' \left(\lfloor \frac{x-a}{\eta'} \rfloor + 1/2\right) \leq \frac{\eta'}{2}$ . Par définition de  $\eta'$ ,  $-\eta \leq a + \eta' \left(\lfloor \frac{x-a}{\eta'} \rfloor + 1/2\right) \leq \eta$ . Par définition de  $\eta$ , on a  $|f(x) - f\left(a + 2\eta \left(\lfloor \frac{x-a}{2\eta} \rfloor + 1/2\right)\right)| \leq \varepsilon$ .

Ainsi, nous avons bien  $\|f - \chi\|_{\infty, [a; b]} \leq \varepsilon$ .

(ii) Écrivons la définition de uniformément continue pour  $\varepsilon$  :

$$\exists \eta \in \mathbb{R}_+^* : \forall (x, y) \in [a; b]^2, |x - y| \leq \eta \implies |f(x) - f(y)| \leq \varepsilon$$

Définissons  $\varphi \in \mathcal{E}([a; b], \mathbb{R})$  par

$$\left| \begin{array}{ll} [a; b] & \rightarrow \mathbb{R} \\ x & \mapsto \begin{cases} f(x) & \text{si } \exists n \in \mathbb{N} : x = a + n\eta \\ \inf f\left(]a + \eta \lfloor \frac{x-a}{\eta'} \rfloor; a + \eta \left(\lfloor \frac{x-a}{\eta'} \rfloor + 1\right)[\right) & \text{sinon} \end{cases} \end{array} \right.$$

Définissons  $\psi \in \mathcal{E}([a; b], \mathbb{R})$  par

$$\left| \begin{array}{ll} [a; b] & \rightarrow \mathbb{R} \\ x & \mapsto \begin{cases} f(x) & \text{si } \exists n \in \mathbb{N} : x = a + n\eta \\ \sup f\left(]a + \eta \lfloor \frac{x-a}{\eta'} \rfloor; a + \eta \left(\lfloor \frac{x-a}{\eta'} \rfloor + 1\right)[\right) & \text{sinon} \end{cases} \end{array} \right.$$

Ces deux fonctions sont bien définies car  $f|_{[a+\eta \lfloor \frac{x-a}{\eta'} \rfloor; a+\eta (\lfloor \frac{x-a}{\eta'} \rfloor + 1)[}$  est continue donc, d'après le théorème de Weierstraß, son image admet une borne inférieure et une borne supérieure. Elle sont bien en escalier.

Par définition des bornes inférieures et supérieures, nous avons  $\varphi \leq f \leq \psi$ . De plus, pour  $x \in [a; b]$  fixé quelconque,  $f|_{[a+\eta \lfloor \frac{x-a}{\eta'} \rfloor; a+\eta (\lfloor \frac{x-a}{\eta'} \rfloor + 1)[}$  se prolonge par continuité et, d'après le théorème de Weierstraß, atteint ses bornes. Notons  $f_i$  et  $f_s$  les antécédents respectifs des bornes.  $(f_i, f_s) \in ]a + \eta \lfloor \frac{x-a}{\eta'} \rfloor; a + \eta (\lfloor \frac{x-a}{\eta'} \rfloor + 1)[^2$  donc  $|f_i - f_s| \leq \eta$ . D'où  $|f(f_i) - f(f_s)| \leq \varepsilon$ .

Ainsi, nous avons bien  $\|\psi - \varphi\|_{\infty, [a; b]} \leq \varepsilon$ . □

## 28 Semaine 30

### 28.7 Dénombrement des surjections de $\llbracket 1; n \rrbracket$ dans $\llbracket 1; 2 \rrbracket$ et dans $\llbracket 1; 3 \rrbracket$

*Démonstration.* Soit  $n \in \mathbb{N}^*$ .

Il y a  $|\llbracket 1; 2 \rrbracket|^{|\llbracket 1; n \rrbracket|} = 2^n$  applications de  $\llbracket 1; n \rrbracket$  dans  $\llbracket 1; 2 \rrbracket$ . Seules les applications constantes  $\tilde{1}$  et  $\tilde{2}$  ne sont pas surjectives. Il y a donc  $2^n - 2$  surjections de  $\llbracket 1; n \rrbracket$  dans  $\llbracket 1; 2 \rrbracket$ .

Il y a  $|\llbracket 1; 3 \rrbracket|^{|\llbracket 1; n \rrbracket|} = 3^n$  applications de  $\llbracket 1; n \rrbracket$  dans  $\llbracket 1; 3 \rrbracket$ . Les applications non surjectives sont celles dont l'image n'est pas  $\llbracket 1; 3 \rrbracket$ . C'est-à-dire, celles dont l'image est de cardinal 1 (les fonctions constantes  $\tilde{1}$ ,  $\tilde{2}$  et  $\tilde{3}$ ) et celles dont l'image est de cardinal 2. Ces dernières sont les surjections de  $\llbracket 1; n \rrbracket$  dans  $\llbracket 1; 2 \rrbracket$ ,  $\{1; 3\}$  et  $\{2; 3\}$ . Comme ces trois ensembles ont la même taille, il y a  $3 \times (2^n - 2)$  (voir résultat précédent) applications de  $\llbracket 1; n \rrbracket$  dans  $\llbracket 1; 3 \rrbracket$  dont l'image est de cardinal 2. Ainsi, le nombre de surjections de  $\llbracket 1; n \rrbracket$  dans  $\llbracket 1; 3 \rrbracket$  est  $3^n - 3 - 3(2^n - 2) = 3^n - 3 \times 2^n + 3$ .  $\square$

### 28.8 Lemme des bergers

Soient  $E, F$  deux ensembles finis non vides et  $f : E \rightarrow F$  telle que tout élément de  $F$  possède le même nombre  $k \in \mathbb{N}^*$  d'antécédents par  $f$ .

Alors  $|F| = \frac{|E|}{k}$

“Pour compter les moutons, il faut compter les pattes puis diviser par quatre. ”

*Démonstration.* Considérons la relation binaire définie sur  $E$  par :

$$\forall (x, y) \in E^2, x \sim y \iff f(x) = f(y)$$

Elle est réflexive, transitive et symétrique donc c'est bien une relation d'équivalence. Donc les classes d'équivalence réalise une partition de  $E$ . Nous avons  $E = \coprod_{C \in E/\sim} C$  donc, en passant aux

cardinaux,  $|E| = \sum_{C \in E/\sim} |C|$ .

Soit  $x \in E$  fixé quelconque. Alors  $\bar{x} = \{y \in E \mid f(x) = f(y)\} = f^{-1}(f(\{x\}))$ . Par hypothèse, tous les éléments de  $F$  ont le même nombre  $k$  d'antécédents, or  $f(x)$  est un singleton d'élément de  $F$  donc  $|\bar{x}| = k$ . Ainsi  $\forall C \in E/\sim, |C| = k$ .

Posons  $\varphi \left| \begin{array}{ccc} E/\sim & \rightarrow & F \\ C & \mapsto & f(x) \text{ où } x \in C \end{array} \right.$   $\cdot$   $\varphi$  est bien défini car si  $(x, y) \in E$  vérifie  $\bar{x} = \bar{y}$  alors  $f(x) = f(y)$  donc l'image par  $\varphi$  ne dépend pas du représentant de classe choisi.  $\varphi$  est surjective car soit  $z \in F$ ,  $f$  est surjective donc  $\exists x_z \in E : f(x_z) = z$  et alors  $\varphi(\bar{x}_z) = f(x_z) = z$ .  $\varphi$  est surjective car soient  $(C, C') \in (E/\sim)^2$ ,  $\varphi(C) = \varphi(C')$  alors  $\exists (x, x') \in C \times C' : x \sim x'$ , comme deux classes d'équivalence sont confondues ou disjointes,  $C = C'$ . Ainsi  $\varphi$  est une bijection donc  $|F| = |E/\sim|$ .

Ainsi  $|E| = \sum_{C \in E/\sim} |C| = \sum_{C \in E/\sim} k = |E/\sim| k = |F| k$ .  $\square$