𝕀𝕏𝟙
Lycée Louis le Grand

2015-2016

Mathématiques

Classe de Mathématiques Supérieures

Cours de Véronique Lods

Notes de Alexis Marchand

Table des matières

Chapitre 1

Complexes

I Définition de $\mathbb{C}$

Définition 1.1 ($\mathbb{C}$). *On définit deux opérations sur* $\mathbb{R}^2$ *(*$(a,b) \in \mathbb{R}^2, (c,d) \in \mathbb{R}^2$*) :*

(i) $(a,b) + (c,d) = (a+c, b+d)$.

(ii) $(a,b) * (c,d) = (ac - bd, ad + bc)$.

On définit aussi la loi externe ($(a,b) \in \mathbb{R}^2, \lambda \in \mathbb{R}$*) :* $\lambda \cdot (a,b) = (\lambda a, \lambda b)$. *On note* $1 = (1,0)$, $i = (0,1)$, $0 = (0,0)$, $\times = *$. *On a* $i \times i = -1$. *On définit alors :*

$$\mathbb{C} = \{a + ib,\ a \in \mathbb{R},\ b \in \mathbb{R}\}.$$

Remarque 1.2. *On dit que* $\mathbb{R} \subset \mathbb{C}$ *au sens où tout réel* a *peut s'écrire* $a + i0$.

Proposition 1.3. $(\mathbb{C}, +)$ *et* $(\mathbb{C}^*, \times)$ *sont des groupes commutatifs.*

Proposition 1.4. *Soit* $\mathcal{P}$ *le plan. L'application*

$$\begin{aligned} \mathbb{C} &\longrightarrow \mathcal{P} \\ a + ib &\longmapsto (a,b) \end{aligned}$$

est une bijection, i.e. tout élément de $\mathcal{P}$ *admet un unique antécédent dans* $\mathbb{C}$.

II Conjugaison et module

II.1 Conjugaison

Définition 1.5. *Soit* $z \in \mathbb{C}$. *On définit* $\overline{z} = \Re(z) - i \cdot \Im(z)$.

Proposition 1.6. $(z, z') \in \mathbb{C}$. $\overline{z} + \overline{z'} = \overline{z + z'}$ *et* $\overline{z} \cdot \overline{z'} = \overline{z \cdot z'}$.

Proposition 1.7.

$$\forall z \in \mathbb{C}, \qquad \Re(z) = \frac{z + \overline{z}}{2} \qquad et \qquad \Im(z) = \frac{z - \overline{z}}{2i}.$$

II.2 Module

Définition 1.8. *Soit $z \in \mathbb{C}$. On définit* $|z| = \sqrt{(\Re(z))^2 + (\Im(z))^2}$.

Proposition 1.9. $\forall (z, z') \in \mathbb{C}^2,\ |zz'| = |z| \cdot |z'|$ *et* $|z|^2 = z\overline{z}$.

Notation 1.10. *Soient $a \in \mathbb{C}, r \in \mathbb{R}_+$. On note :*

$$\begin{aligned} D_f(a,r) &= \{z \in \mathbb{C},\ |z-a| \leqslant r\}, \\ D_o(a,r) &= \{z \in \mathbb{C},\ |z-a| < r\}, \\ \mathcal{C}(a,r) &= \{z \in \mathbb{C},\ |z-a| = r\}. \end{aligned}$$

Proposition 1.11 (Inégalité triangulaire)**.**

$$\forall (a,b) \in \mathbb{C}^2,\ |a+b| \leqslant |a| + |b|,$$

avec égalité ssi *les points d'affixes a et b sont sur une même demi-droite issue de l'origine (i.e. pour $a \neq 0, b \neq 0$: $\arg a \equiv \arg b \quad [2\pi]$).*

Démonstration. On a $|a+b|^2 = (a+b)\left(\overline{a} + \overline{b}\right) = |a|^2 + |b|^2 + 2\Re(a\overline{b}) \leqslant |a|^2 + |b|^2 + 2|a||b| = (|a| + |b|)^2$. □

Corollaire 1.12. $\forall (z, z') \in \mathbb{C}^2,\ ||z| - |z'|| \leqslant |z - z'|$.

III Étude de $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$

Proposition 1.13. $(\mathbb{U}, \times)$ *est un groupe commutatif dit groupe unité.*

Proposition 1.14. $(z, z') \in (\mathbb{C}^*)^2$.

$$\arg(zz') \equiv \arg z + \arg z' \quad [2\pi], \tag{i}$$

$$\arg\left(\frac{1}{z}\right) \equiv -\arg z \quad [2\pi]. \tag{ii}$$

Proposition 1.15. *Soient A, B, C trois points d'affixes respectives a, b, c distinctes deux à deux. Alors*

$$A,\ B,\ C \text{ sont alignés} \quad \Longleftrightarrow \quad \arg\left(\frac{c-a}{b-a}\right) \equiv 0 \quad [\pi].$$

IV Identités remarquables

Théorème 1.16 (Formule du binôme de Newton)**.** $(z, z') \in \mathbb{C}^2$, $n \in \mathbb{N}$.

$$(z+z')^n = \sum_{k=0}^{n} \binom{n}{k} z^k z'^{n-k}.$$

Démonstration. Fixer z et z' dans $\mathbb{C}$ et utiliser une récurrence sur n. □

Proposition 1.17. $(z, z') \in \mathbb{C}^2$, $n \in \mathbb{N}^*$.

$$z^n - z'^n = (z - z') \sum_{k=0}^{n-1} z^k z'^{n-1-k}.$$

Démonstration. Développer $(z-z')\sum_{k=0}^{n-1} z^k z'^{n-1-k}$. □

Proposition 1.18 (Somme géométrique)**.** $z \in \mathbb{C}$, $n \in \mathbb{N}$.

$$\sum_{k=0}^{n} z^k = \begin{cases} \frac{z^{n+1}-1}{z-1} & si\ z \neq 1 \\ n+1 & si\ z = 1 \end{cases}.$$

Démonstration. Développer $(z-1)\sum_{k=0}^{n} z^k$. □

V Propriétés de la forme exponentielle

Proposition 1.19. $\forall (\theta, \phi) \in \mathbb{R}^2,\ e^{i\theta} = e^{i\phi} \iff \theta \equiv \phi \quad [2\pi]$.

Proposition 1.20 (Formules d'Euler)**.** $\theta \in \mathbb{R}$.

$$\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2} \qquad et \qquad \sin\theta = \frac{e^{i\theta}-e^{-i\theta}}{2i}.$$

Proposition 1.21 (Formules de l'angle moitié)**.** $(\theta, \phi) \in \mathbb{R}^2$.

$$e^{i\theta} + e^{i\phi} = 2\cos\left(\frac{\theta-\phi}{2}\right) e^{i\frac{\theta+\phi}{2}}, \tag{i}$$

$$e^{i\theta} - e^{i\phi} = 2i\sin\left(\frac{\theta-\phi}{2}\right) e^{i\frac{\theta+\phi}{2}}. \tag{ii}$$

Corollaire 1.22 (Formule de Moivre)**.** $n \in \mathbb{Z}$, $\theta \in \mathbb{R}$. $\left(e^{i\theta}\right)^n = e^{in\theta}$, *soit*

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).$$

Notation 1.23. *On note* $j = e^{i\frac{2\pi}{3}}$. *On a alors* $j^3 = 1$ *et* $1 + j + j^2 = 0$.

Proposition 1.24 (Linéarisation de $\cos^n\theta$)**.** $n \in \mathbb{N}^*$, $\theta \in \mathbb{R}$.

$$\cos^n\theta = \left(\frac{e^{i\theta}+e^{-i\theta}}{2}\right)^n = \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}\cos\left[(2k-n)\theta\right].$$

Proposition 1.25 (Somme des $\cos(k\theta)$)**.** $n \in \mathbb{N}^*$, $\theta \in \mathbb{R}$.

$$\sum_{k=0}^{n}\cos(k\theta) = \Re\left(\sum_{k=0}^{n}\left(e^{i\theta}\right)^k\right) = \frac{\cos\left(\frac{n\theta}{2}\right)\sin\left(\frac{(n+1)\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}.$$

VI Aspect géométrique

Proposition 1.26 (Équation d'une droite en complexes)**.** *Soient A le point du plan d'affixe a,* $\vec{u}$ *le vecteur d'affixe u (avec* $\vec{u} \neq \vec{0}$*) et M le point d'affixe z. Alors M appartient à la droite passant par A et dirigée par* $\vec{u}$ ssi $\overline{u}(z-a) = u(\overline{z}-\overline{a})$.

Proposition 1.27 (Transformations du plan)**.** *Soient* $\vec{u}$ *un vecteur du plan d'affixe u,* Ω *un point d'affixe* ω, θ *et k des réels. Alors*

(i) *L'application* $\tau_{\vec{u}} : M(z) \longmapsto M'(z+u)$ *est une* translation *de vecteur* $\vec{u}$.

(ii) *L'application* $\rho_{\Omega,\theta} : M(z) \longmapsto M'(\omega + e^{i\theta}(z-\omega))$ *est une* rotation *de centre* Ω *et d'angle* θ.

(iii) *L'application* $h_{\Omega,k} : M(z) \longmapsto M'(\omega + k(z-\omega))$ *est une* homothétie *de centre* Ω *et de rapport* k.

Définition 1.28 (Similitude)**.** *On dit que* $f : \mathcal{P} \longrightarrow \mathcal{P}$ *est une* similitude *de rapport* k *lorsque*

$$\forall (M,N) \in \mathcal{P}^2,\ f(M)f(N) = kMN.$$

Soit $(a,b) \in \mathbb{C}^* \times \mathbb{C}$. *Alors*

$$M(z) \longmapsto M'(az+b) \text{ est une similitude directe.} \tag{i}$$

$$M(z) \longmapsto M'(a\overline{z}+b) \text{ est une similitude indirecte.} \tag{ii}$$

Proposition 1.29. *Soit* $f : M(z) \longmapsto M'(az+b)$, *avec* $(a,b) \in \mathbb{C}^2$, $a \neq 0$ *et* $a \neq 1$. *Alors* f *est la composée, dans un ordre quelconque, d'une homothétie et d'une rotation de même centre.*

Démonstration. On recherche $\Omega(\omega)$ tel que $f(\Omega) = \Omega$, soit $\omega = a\omega + b$, i.e. $\omega = \frac{b}{1-a}$. On note z l'affixe d'un point M et z' l'affixe de $f(M)$. On a alors $z' - \omega = (az+b) - (a\omega+b) = a(z-\omega) = |a|e^{i\theta}(z-\omega)$, où $\theta = \arg a$. On pose $h = h_{\Omega,|a|}$ et $r = \rho_{\Omega,\theta}$. On montre alors par le calcul que $f = h \circ r = r \circ h$. □

VII Exponentielle complexe

Définition 1.30 (Exponentielle complexe)**.** *On définit l'application*

$$\exp : \left| \begin{array}{l} \mathbb{C} \longrightarrow \mathbb{C}^* \\ z \longmapsto e^{\Re(z)} \cdot e^{i\Im(z)} \end{array} \right. .$$

On notera $e^z = \exp z$.

Proposition 1.31. $(z,z') \in \mathbb{C}^2$.

$$|e^z| = e^{\Re(z)}, \tag{i}$$

$$\arg e^z \equiv \Im(z) \quad [2\pi], \tag{ii}$$

$$e^z e^{z'} = e^{z+z'}. \tag{iii}$$

VIII Équations du second degré

VIII.1 Résolution de $z^2 = d$, où $d \in \mathbb{C}$

Proposition 1.32. *Soit* $d \in \mathbb{C}$. *Alors*

$$\text{L'équation } z^2 = d \text{ a } \left\{ \begin{array}{l} \text{1 solution dans } \mathbb{C} \text{ si } d = 0 \\ \text{2 solutions dans } \mathbb{C} \text{ si } d \neq 0 \end{array} \right. .$$

Méthode 1.33. *Pour résoudre* $z^2 = d$, *on pose* $z = x+iy$ *et* $d = X+iY$, *avec* $(x,y) \in \mathbb{R}^2$, $(X,Y) \in \mathbb{R}^2$. *On a ainsi :*

$$z^2 = d \Longleftrightarrow \left\{ \begin{array}{l} x^2 - y^2 = X \\ 2xy = Y \\ x^2 + y^2 = \sqrt{X^2+Y^2} \end{array} \right. \Longleftrightarrow \left\{ \begin{array}{l} x^2 = \frac{\sqrt{X^2+Y^2}+X}{2} \\ 2xy = Y \\ y^2 = \frac{\sqrt{X^2+Y^2}-X}{2} \end{array} \right. .$$

On peut alors déduire les valeurs de x *et* y.

VIII.2 Résolution de $az^2+bz+c=0$, où $(a,b,c)\in\mathbb{C}^*\times\mathbb{C}\times\mathbb{C}$

Proposition 1.34. *Soit $(a,b,c)\in\mathbb{C}^*\times\mathbb{C}\times\mathbb{C}$; on note (E) l'équation $az^2+bz+c=0$. On pose $\Delta=b^2-4ac$.*

(i) *Si $\Delta=0$, alors (E) a une unique racine : $-\frac{b}{2a}$.*

(ii) *Si $\Delta\neq 0$, alors (E) a exactement deux racines distinctes : $\frac{-b+\delta}{2a}$ et $\frac{-b-\delta}{2a}$, où δ est un complexe tel que $\delta^2=\Delta$.*

Démonstration. On a $az^2+bz+c=0\iff\left(z+\frac{b}{2a}\right)^2=\left(\frac{\delta}{2a}\right)^2$. □

Proposition 1.35. *On note (E) l'équation $az^2+bz+c=0$, avec $(a,b,c)\in\mathbb{C}^*\times\mathbb{C}\times\mathbb{C}$.*

$$z_1 \text{ et } z_2 \text{ sont les racines de } (E)\iff\begin{cases} z_1+z_2=-\frac{b}{a} \\ z_1\cdot z_2=\frac{c}{a}\end{cases}, \tag{i}$$

$$\forall z\in\mathbb{C},\ az^2+bz+c=a(z-z_1)(z-z_2)\ (z_1,\ z_2 \text{ racines de } (E)), \tag{ii}$$

$$(a,b,c)\in\mathbb{R}^3\Longrightarrow (E) \text{ admet deux racines } \begin{cases} \text{conjuguées si } \Delta<0 \\ \text{réelles si } \Delta\geqslant 0\end{cases}. \tag{iii}$$

IX Racines n-ièmes

Notation 1.36. *Pour $k\in\mathbb{Z}$, on note $\omega_k=e^{k\cdot\frac{2i\pi}{n}}=\omega^k$, avec $\omega=\omega_1$. On note aussi*

$$\mathbb{U}_n=\{\omega_k,\ k\in[\![0,n-1]\!]\}.$$

IX.1 Propriétés de ω_k

Proposition 1.37. *Soit $X_n=\{\omega_k,k\in\mathbb{Z}\}$. Alors :*

(i) *X_n présente une symétrie axiale par rapport à (Ox).*

(ii) *Pour n pair, X_n présente aussi une symétrie axiale par rapport à (Oy) et une symétrie centrale par rapport à O.*

(iii) *Les points d'affixes $1,\omega,\ldots,\omega_{n-1}$ sont les sommets d'un n-gône régulier.*

Proposition 1.38. $n\in\mathbb{N}^*$.

$$\sum_{k=0}^{n-1}\omega_k=\begin{cases}0 & si\ n\neq 1\\ 1 & si\ n=1\end{cases}, \tag{i}$$

$$\prod_{k=0}^{n-1}\omega_k=(-1)^{n-1}. \tag{ii}$$

IX.2 Propriétés de $\mathbb{U}_n$

Théorème 1.39 (Division euclidienne)**.** $(a,b)\in\mathbb{Z}\times\mathbb{N}^*$.

$$\exists!(q,r)\in\mathbb{Z}^2,\ \begin{cases} a=bq+r\\ 0\leqslant r<b\end{cases}.$$

Démonstration. On pose $q=\left\lfloor\frac{a}{b}\right\rfloor$ (où $\lfloor x\rfloor$ désigne la partie entière de x), et $r=a-bq$. q et r vérifient alors la condition voulue ; il suffit de montrer l'unicité en supposant que deux couples différents (q,r) et (q',r') existent, et arriver à $q=q'$ et $r=r'$. □

Proposition 1.40. (i) *$\mathbb{U}_n$ a exactement n éléments,*

(ii) *$\mathbb{U}_n=X_n=\{\omega_k,\ k\in\mathbb{Z}\}$.*

IX.3 Racines n-ièmes d'un complexe

Définition 1.41 (Racines n-ièmes)**.** *Soient $Z \in \mathbb{C}, n \in \mathbb{N}^*$. On appelle racine n-ième de Z tout complexe z tel que $z^n = Z$.*

Proposition 1.42. *L'ensemble des racines n-ièmes de l'unité est $\mathbb{U}_n$.*

Proposition 1.43. $n \in \mathbb{N}^*, z \in \mathbb{C}$. $\prod_{k=0}^{n-1} (z - \omega_k) = z^n - 1$.

Chapitre 2

Logique

I Vocabulaire

Définition 2.1. *On appelle* assertion *toute phrase mathématique syntaxiquement correcte (ex : $2 = 1 + 3$). On appelle* prédicat *toute assertion mathématique dépendant d'une ou plusieurs variables (ex : $x \in \mathbb{R}_+, \mathcal{P}(x) : x \geqslant 1$).*

Définition 2.2 (Connecteurs logiques et implications)**.** *A, B deux assertions. On définit les assertions (A et B), (A ou B), (non A) et ($A \Rightarrow B$) par la table de vérité suivante :*

A	B	A et B	A ou B	non A	$A \Rightarrow B$
V	V	V	V	F	V
V	F	F	V	F	F
F	V	F	V	V	V
F	F	F	F	V	V

Proposition 2.3. *A, B deux assertions.*

$$(\text{non } [A \text{ ou } B]) \iff ([\text{non } A] \text{ et } [\text{non } B]), \tag{i}$$

$$(\text{non } [A \text{ et } B]) \iff ([\text{non } A] \text{ ou } [\text{non } B]), \tag{ii}$$

$$(A \Rightarrow B) \iff ([\text{non } A] \text{ ou } B), \tag{iii}$$

$$(\text{non } [A \Rightarrow B]) \iff (A \text{ et } [\text{non } B]). \tag{iv}$$

Vocabulaire 2.4. *A, B deux assertions telles que $A \Rightarrow B$. A est une* condition suffisante *(CS) pour B. Et B est une* condition nécessaire *(CN) pour A.*

II Quantificateurs

Définition 2.5. *E un ensemble non vide, $\mathcal{P}(x)$ un prédicat pour $x \in E$. On note :*

(i) *$\forall x \in E,\ \mathcal{P}(x)$ pour signifier que pour tout $x \in E$, $\mathcal{P}(x)$ est vraie.*

(ii) *$\exists x \in E,\ \mathcal{P}(x)$ pour signifier qu'il existe un $x \in E$ tel que $\mathcal{P}(x)$ est vraie.*

(iii) *$\exists! x \in E,\ \mathcal{P}(x)$ pour signifier qu'il existe un unique $x \in E$ tel que $\mathcal{P}(x)$ est vraie.*

Proposition 2.6. *E un ensemble non vide, $\mathcal{P}(x)$ un prédicat pour $x \in E$.*

$$(\text{non } [\forall x \in E,\ \mathcal{P}(x)]) \iff (\exists x \in E,\ [\text{non } \mathcal{P}(x)]), \tag{i}$$

$$(\text{non } [\exists x \in E,\ \mathcal{P}(x)]) \iff (\forall x \in E,\ [\text{non } \mathcal{P}(x)]). \tag{ii}$$

III Raisonnements élémentaires

Proposition 2.7 (Contre-exemple)**.** *E un ensemble non vide, $\mathcal{P}(x)$ un prédicat pour $x \in E$. Pour montrer que l'assertion $(\forall x \in E,\ \mathcal{P}(x))$ est fausse, il suffit de chercher un $x \in E$ tel que $(\text{non } \mathcal{P}(x))$ est vraie.*

Proposition 2.8 (Contraposée)**.** *A, B deux assertions.*

$$(A \Rightarrow B) \iff ([\text{non } B] \Rightarrow [\text{non } A])\,.$$

Démonstration. Utiliser $(A \Rightarrow B) \iff ([\text{non } A] \text{ ou } B)$. □

Proposition 2.9 (Raisonnement par l'absurde)**.** *A une assertion. Pour montrer que A est vraie, on suppose que A est fausse et on aboutit à une contradiction.*

IV Raisonnements par récurrence

Axiome 2.10 (Axiomes de Peano)**.** *On suppose qu'il existe un ensemble noté $\mathbb{N}$, un élément $0 \in \mathbb{N}$ et une application $s : n \in \mathbb{N} \longmapsto$ successeur de n tels que :*

(i) *0 n'est le successeur d'aucun élément de $\mathbb{N}$,*

(ii) *Deux éléments de $\mathbb{N}$ distincts ont des successeurs distincts,*

(iii) *Pour tout $A \subset \mathbb{N}$, si $0 \in A$ et $\forall a \in A,\ s(a) \in A$, alors $A = \mathbb{N}$.*

Corollaire 2.11 (Récurrence)**.** *$\mathcal{P}(n)$ une propriété définie pour $n \in \mathbb{N}$.*

$$\left.\begin{array}{r} \mathcal{P}(0) \text{ est vraie} \\ \forall n \in \mathbb{N},\ \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1) \end{array}\right\} \Longrightarrow \forall n \in \mathbb{N},\ \mathcal{P}(n).$$

Proposition 2.12 (Récurrence à deux termes)**.** *$\mathcal{P}(n)$ une propriété définie pour $n \in \mathbb{N}$.*

$$\left.\begin{array}{r} \mathcal{P}(0) \text{ et } \mathcal{P}(1) \text{ sont vraies} \\ \forall n \in \mathbb{N},\ (\mathcal{P}(n) \text{ et } \mathcal{P}(n+1)) \Rightarrow \mathcal{P}(n+2) \end{array}\right\} \Longrightarrow \forall n \in \mathbb{N},\ \mathcal{P}(n).$$

Démonstration. Poser $\mathcal{Q}(n) = (\mathcal{P}(n) \text{ et } \mathcal{P}(n+1))$. □

Proposition 2.13 (Récurrence forte)**.** *$\mathcal{P}(n)$ une propriété définie pour $n \in \mathbb{N}$.*

$$\left.\begin{array}{r} \mathcal{P}(0) \text{ est vraie} \\ \forall n \in \mathbb{N},\ (\mathcal{P}(0) \text{ et } \cdots \text{ et } \mathcal{P}(n)) \Rightarrow \mathcal{P}(n+1) \end{array}\right\} \Longrightarrow \forall n \in \mathbb{N},\ \mathcal{P}(n).$$

Démonstration. Poser $\mathcal{Q}(n) = (\mathcal{P}(0) \text{ et } \cdots \text{ et } \mathcal{P}(n))$. □

Proposition 2.14 (Récurrence descendante)**.** *$n_0 \in \mathbb{Z}$, $\mathcal{P}(n)$ une propriété définie pour $n \in [\![-\infty, n_0]\!]$.*

$$\left.\begin{array}{r} \mathcal{P}(n_0) \text{ est vraie} \\ \forall n \leqslant n_0,\ \mathcal{P}(n) \Rightarrow \mathcal{P}(n-1) \end{array}\right\} \Longrightarrow \forall n \leqslant n_0,\ \mathcal{P}(n).$$

V Vocabulaire ensembliste

Définition 2.15 (Ensemble)**.** *Un* ensemble *est une collection d'objets. Un ensemble sans objet est dit* ensemble vide*, noté* $\varnothing$*. Un ensemble ne contenant qu'un seul élément est dit* singleton*. Soit a un objet d'un ensemble E. On dit que a est un* élément *de E, et on note $a \in E$.*

Notation 2.16. *Un ensemble E ayant n éléments $a_1, \dots, a_n$ ($n \in \mathbb{N}^*$) est noté :*

$$E = \{a_1, \dots, a_n\} = \{a_i,\ i \in [\![1, n]\!]\}\,.$$

Définition 2.17 (Inclusion)**.** *E, F deux ensembles. On dit que E est inclus dans F, et on note $E \subset F$, lorsque tout élément de E appartient à F.*

Définition 2.18 (Égalité)**.** *E, F deux ensembles. On dit que E et F sont égaux, et on note $E = F$, lorsque E et F ont les mêmes éléments (i.e. $E \subset F$ et $E \supset F$).*

Notation 2.19. *L'ensemble des* parties *(ou sous-ensembles) d'un ensemble F est noté $\mathcal{P}(F)$.*

Proposition 2.20. *Soit F un ensemble à n éléments ($n \in \mathbb{N}$). Alors $\mathcal{P}(F)$ est un ensemble à 2^n éléments.*

Démonstration. $\binom{n}{k}$ est le nombre de parties de F à k éléments donc le nombre de parties de F est $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. □

Définition 2.21 (Segment)**.** $(a, b) \in \mathbb{C}^2$*. Le* segment $[a, b]$ *est défini par*

$$[a, b] = \{\lambda a + (1 - \lambda)b,\ \lambda \in [0, 1]\}\,.$$

On définit de même $]a, b]$, $[a, b[$ et $]a, b[$.

Définition 2.22 (Opérations ensemblistes)**.** *A, B deux sous-ensembles d'un ensemble E. On note :*

(i) *$A \cup B$ l'ensemble des éléments qui appartiennent à A ou à B,*

(ii) *$A \cap B$ l'ensemble des éléments qui appartiennent à A et à B.*

Proposition 2.23. *$\cup$ et $\cap$ sont des opérations sur $\mathcal{P}(E)$, et on a :*

(i) *$\cup$ et $\cap$ sont associatives et commutatives.*

(ii) *$\varnothing$ est l'élément neutre pour $\cup$; E est l'élément neutre pour $\cap$.*

(iii) *$\cup$ est distributive sur $\cap$ et $\cap$ est distributive sur $\cup$.*

Notation 2.24. *$I \subset \mathbb{N}$, $I \neq \varnothing$. $(A_i)_{i \in I}$ une famille de sous-ensembles d'un ensemble E. On note :*

$$\bigcup_{i \in I} A_i = \{x \in E,\ \exists i \in I,\ x \in A_i\}\,, \tag{i}$$

$$\bigcap_{i \in I} A_i = \{x \in E,\ \forall i \in I,\ x \in A_i\}\,. \tag{ii}$$

Définition 2.25 (Complémentaire)**.** *E un ensemble, $A \subset E, B \subset E$. On note $\overline{A}$ l'ensemble des éléments de E qui ne sont pas dans A. On note $A \backslash B = A \cap \overline{B}$.*

Proposition 2.26 (Lois de Morgan)**.** *$I \subset \mathbb{N}$, $I \neq \varnothing$. $(A_i)_{i\in I}$ une famille de sous-ensembles d'un ensemble E.*

$$\overline{\bigcup_{i\in I} A_i} = \bigcap_{i\in I} \overline{A_i} \qquad et \qquad \overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A_i}.$$

Démonstration. Écrire $x \in \overline{\bigcup_{i\in I} A_i} \iff$ non $(\exists i \in I,\ x \in A_i) \iff \forall i \in I,\ x \notin A_i \iff x \in \bigcap_{i\in I} \overline{A_i}$. Puis poser $B_i = \overline{A_i}$ pour montrer la deuxième égalité à partir de la première. □

Définition 2.27 (Produit cartésien)**.** *Le* produit cartésien *de n ensembles $E_1, \ldots, E_n$ ($n \in \mathbb{N}^*$) est défini par*

$$E_1 \times \cdots \times E_n = \{(x_1, \ldots, x_n),\ \forall i \in [\![1, n]\!],\ x_i \in E_i\}.$$

Si $E_1 = \cdots = E_n$, on note $E_1 \times \cdots \times E_n = (E_1)^n$.

Chapitre 3

Applications et Relations

I Notions élémentaires

Définition 3.1 (Application)**.** *E, F deux ensembles (non vides). Soit G un sous-ensemble de $E \times F$ t.q. $\forall a \in E$, $\exists! b \in F$, $(a, b) \in G$. Dans ce cas, on peut associer à tout élément de E un* unique élément *dans F, et on note $f : E \to F$ dite* application de E dans F *définie de telle sorte que pour tout $a \in E$, $f(a)$ est l'unique élément de F tel que $(a, f(a)) \in G$. G est dit le* graphe *de f.*

Corollaire 3.2. *Deux applications f et g sont dites égales lorsque :*

$$\begin{cases} f \text{ et } g \text{ ont le même ensemble de départ } E \\ f \text{ et } g \text{ ont le même ensemble d'arrivée } F \\ f \text{ et } g \text{ ont le même graphe } G \end{cases}.$$

Vocabulaire 3.3. *$f : E \to F$ une application.*

(i) *L'*image *d'un élément $x \in E$ est $f(x)$.*

(ii) *Un* antécédent *d'un élément $y \in F$ est un élément $x \in E$ t.q. $f(x) = y$.*

(iii) *L'*ensemble image *de E par f est $f(E) = \{f(x),\ x \in E\} \subset F$.*

Définition 3.4. *E, F des ensembles non vides, $f : E \to F$ une application, $E' \subset E$ et $E'' \supset E$.*

(i) *On appelle* identité *de E l'application $id_E : \left| \begin{array}{l} E \longrightarrow E \\ x \longmapsto x \end{array} \right.$.*

(ii) *On appelle* restriction *de f à E' l'application $f_{|E'} : \left| \begin{array}{l} E' \longrightarrow F \\ x \longmapsto f(x). \end{array} \right.$*

(iii) *On appelle* prolongement *de f à E'' toute application $\phi : E'' \to F$ t.q.*

$$\forall x \in E,\ \phi(x) = f(x).$$

Définition 3.5 (Composée)**.** *$f : E \to F$, $g : F \to G$. On définit la* composée *$g \circ f$ par*

$$g \circ f : \left| \begin{array}{l} E \longrightarrow G \\ x \longmapsto g(f(x)) \end{array} \right..$$

Notation 3.6. *L'ensemble des applications de E dans F est noté $\mathcal{F}(E, F)$ ou F^E.*

Proposition 3.7 (Associativité de $\circ$)**.** *$f : E \to F$, $g : F \to G$ et $h : G \to H$.*

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

II Injectivité, surjectivité, bijectivité

II.1 Applications injectives

Définition 3.8 (Injectivité)**.** *$f : E \to F$. L'application f est dite* injective *lorsque*

$$\forall (x, x') \in E^2,\ \left[f(x) = f(x') \Longrightarrow x = x' \right],$$

i.e. tout élément de F a au plus un antécédent dans E.

Proposition 3.9. *Toute restriction d'une application injective est injective.*

Proposition 3.10. *$f : E \to F$, $g : F \to G$.*

$$\left.\begin{array}{l} f \text{ injective} \\ g \text{ injective} \end{array}\right\} \Longrightarrow g \circ f \text{ injective}, \tag{i}$$

$$g \circ f \text{ injective} \Longrightarrow f \text{ injective}. \tag{ii}$$

II.2 Applications surjectives

Définition 3.11 (Surjectivité)**.** *$f : E \to F$. L'application f est dite* surjective *lorsque*

$$\forall y \in F,\ \exists x \in E,\ y = f(x),$$

i.e. tout élément de F a au moins un antécédent dans E.

Remarque 3.12. *La restriction d'une application surjective n'est pas forcément surjective.*

Proposition 3.13. *$f : E \to F$, $g : F \to G$.*

$$\left.\begin{array}{l} f \text{ surjective} \\ g \text{ surjective} \end{array}\right\} \Longrightarrow g \circ f \text{ surjective}, \tag{i}$$

$$g \circ f \text{ surjective} \Longrightarrow g \text{ surjective}. \tag{ii}$$

II.3 Applications bijectives

Définition 3.14 (Bijection)**.** *$f : E \to F$. L'application f est dite* bijection *de E sur F lorsque tout élément de F admet un unique antécédent dans E, i.e. f est injective et surjective.*

Proposition 3.15. *$f : E \to F$.*

$$f \text{ bijective} \Longleftrightarrow \exists g \in E^F,\ \left\{ \begin{array}{l} g \circ f = id_E \\ f \circ g = id_F \end{array} \right. .$$

De plus, g est unique. On note $g = f^{-1}$.

Définition 3.16 (Involution)**.** *Une application $f : E \to E$ est dite* involutive *lorsque $f \circ f = id_E$.*

Proposition 3.17. *Toute involution est bijective de réciproque elle-même.*

Proposition 3.18. *$f : E \to F$, $g : F \to G$.*

$$\left.\begin{array}{r} f \text{ bijective} \\ g \text{ bijective} \end{array}\right\} \Longrightarrow g \circ f \text{ bijective}, \tag{i}$$

$$\left.\begin{array}{r} f \text{ bijective} \\ g \text{ bijective} \end{array}\right\} \Longrightarrow (g \circ f)^{-1} = f^{-1} \circ g^{-1}. \tag{ii}$$

Notation 3.19. *E un ensemble. On note $\mathcal{G}(E)$ l'ensemble des bijections de E sur E.*

Proposition 3.20. *$(\mathcal{G}(E), \circ)$ est un groupe.*

II.4 Injectivité, surjectivité, bijectivité et ensembles finis

Proposition 3.21. *E, F des ensembles. $f : E \to F$ une application.*

$$\left.\begin{array}{r} E \text{ un ensemble fini} \\ f \text{ injective} \end{array}\right\} \Longrightarrow F \text{ est infini ou a plus d'éléments que } E, \tag{i}$$

$$\left.\begin{array}{r} F \text{ un ensemble fini} \\ f \text{ surjective} \end{array}\right\} \Longrightarrow E \text{ est infini ou a plus d'éléments que } F. \tag{ii}$$

Proposition 3.22. *E, F des ensembles finis avec le même nombre d'éléments. $f : E \to F$ une application. Alors*

$$f \text{ injective} \Longleftrightarrow f \text{ surjective} \Longleftrightarrow f \text{ bijective}.$$

III Applications caractéristiques

Définition 3.23 (Application caractéristique)**.** *E un ensemble non vide. $A \subset E$. On appelle* application caractéristique *(ou indicatrice) de A l'application*

$$\mathbb{1}_A : \left| \begin{array}{l} E \longrightarrow \{0,1\} \\ x \longmapsto \left\{ \begin{array}{l} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{array} \right. \end{array} \right. .$$

Proposition 3.24. *L'application* $\left| \begin{array}{l} \mathcal{P}(E) \longrightarrow \{0,1\}^E \\ A \longmapsto \mathbb{1}_A \end{array} \right.$ *est une bijection.*

Notation 3.25. *A, B deux sous-ensembles d'un ensemble E. On note*

$$\mathbb{1}_A + \mathbb{1}_B : \left| \begin{array}{l} E \longrightarrow \{0,1,2\} \\ x \longmapsto \mathbb{1}_A(x) + \mathbb{1}_B(x) \end{array} \right. \quad \text{et} \quad \mathbb{1}_A - \mathbb{1}_B : \left| \begin{array}{l} E \longrightarrow \{-1,0,1\} \\ x \longmapsto \mathbb{1}_A(x) - \mathbb{1}_B(x) \end{array} \right. .$$

Proposition 3.26. *A, B deux sous-ensembles d'un ensemble E.*

$$\mathbb{1}_{A \cap B} = \mathbb{1}_A \cdot \mathbb{1}_B, \tag{i}$$

$$\mathbb{1}_{A \cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \cdot \mathbb{1}_B, \tag{ii}$$

$$\mathbb{1}_{B \setminus A} = \mathbb{1}_B - \mathbb{1}_A \text{ (si } A \subset B). \tag{iii}$$

Définition 3.27 (Différence symétrique)**.** *A, B deux sous-ensembles d'un ensemble E. On définit la* différence symétrique $\triangle$ *comme suit :*

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

Proposition 3.28. $\mathbb{1}_{A \triangle B} = \mathbb{1}_A + \mathbb{1}_B - 2 \cdot \mathbb{1}_A \cdot \mathbb{1}_B$.

Proposition 3.29. *$(\mathcal{P}(E), \triangle)$ est un groupe commutatif.*

Proposition 3.30. *$\cap$ est distributive par rapport à $\triangle$: $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.*

IV Images directes et réciproques

IV.1 Image directe

Définition 3.31 (Image directe)**.** *E, F deux ensembles non vides. $f : E \to F$. Pour $A \subset E$, on appelle* image directe *de A par f, notée $f(A)$, l'ensemble des images des éléments de A par f :*

$$f(A) = \{f(a),\, a \in A\}.$$

Proposition 3.32. *$f : E \to F$. $(A, B) \in \mathcal{P}(E)^2$.*

$$f(A \cup B) = f(A) \cup f(B), \tag{i}$$

$$f(A \cap B) \subset f(A) \cap f(B). \tag{ii}$$

Proposition 3.33. *$f : E \to F$. $(A, B) \in \mathcal{P}(E)^2$. Si f est injective, alors*

$$f(A) = f(B) \Longrightarrow A = B.$$

Proposition 3.34. *$f : E \to F$. $g : F \to G$. $A \subset E$.*

$$(g \circ f)(A) = g(f(A)).$$

IV.2 Image réciproque

Définition 3.35 (Image réciproque)**.** *E, F deux ensembles non vides. $f : E \to F$. Pour $B \subset F$, on appelle* image réciproque *de B par f, notée $f^*(B)$ ou $f^{-1}(B)$, l'ensemble des antécédents des éléments de B par f :*

$$f^*(B) = \{x \in E,\, f(x) \in B\}.$$

Proposition 3.36. *Soit $f : E \to F$ une application bijective, $(A, B) \in \mathcal{P}(E)^2$.*

$$f(A) = B \Longleftrightarrow A = f^*(B).$$

Proposition 3.37. *$f : E \to F$. $(A, B) \in \mathcal{P}(F)^2$.*

$$f^*(A \cup B) = f^*(A) \cup f^*(B), \tag{i}$$

$$f^*(A \cap B) = f^*(A) \cap f^*(B). \tag{ii}$$

IV.3 Partie stable

Définition 3.38 (Stabilité)**.** *$f : E \to F$. $A \subset E$. A est dit* stable *par f lorsque $f(A) \subset A$.*

V Relations sur un ensemble

V.1 Généralités

Définition 3.39 (Relation binaire)**.** *Soit E un ensemble, $G \subset E \times E$. Alors G définit une* relation binaire *$\mathcal{R}$ sur E définie par $x\mathcal{R}y \Longleftrightarrow (x, y) \in G$.*

Définition 3.40 (Réflexivité, symétrie, transitivité)**.** *Soit $\mathcal{R}$ une relation sur un ensemble E.*

(i) $\mathcal{R}$ *est* réflexive *si* $\forall x \in E,\ x\mathcal{R}x$.

(ii) $\mathcal{R}$ *est* symétrique *si* $\forall (x,y) \in E^2,\ (x\mathcal{R}y \Longrightarrow y\mathcal{R}x)$.

(iii) $\mathcal{R}$ *est* antisymétrique *si* $\forall (x,y) \in E^2,\ (x\mathcal{R}y \text{ et } y\mathcal{R}x \Longrightarrow x = y)$.

(iv) $\mathcal{R}$ *est* transitive *si* $\forall (x,y,z) \in E^3,\ (x\mathcal{R}y \text{ et } y\mathcal{R}z \Longrightarrow x\mathcal{R}z)$.

Définition 3.41 (Ordre, équivalence)**.** *Soit $\mathcal{R}$ une relation sur un ensemble E.*

(i) $\mathcal{R}$ *est une* relation d'équivalence *si $\mathcal{R}$ est réflexive, symétrique et transitive.*

(ii) $\mathcal{R}$ *est une* relation d'ordre *si $\mathcal{R}$ est réflexive, antisymétrique et transitive.*

V.2 Relations d'ordre

Définition 3.42 (Ordre total ou partiel)**.** *Soit $\mathcal{R}$ une relation d'ordre sur un ensemble E.*

(i) *Deux éléments a et b de E sont* comparables *si $a\mathcal{R}b$ ou $b\mathcal{R}a$.*

(ii) $\mathcal{R}$ *est une* relation d'ordre total *sur E si tous les éléments de E sont comparables.*

(iii) $\mathcal{R}$ *est une* relation d'ordre partiel *sur E si $\mathcal{R}$ n'est pas une relation d'ordre total.*

Exemple 3.43 (Ordre lexicographique)**.** *L'*ordre lexicographique *défini dans $\mathbb{R}^2$ par*

$$(x,y) \prec (x',y') \Longleftrightarrow \left[(x < x') \text{ ou } (x = x' \text{ et } y \leqslant y')\right]$$

est une relation d'ordre total.

Définition 3.44 (Majorant, minorant, etc.)**.** *$\lhd$ une relation d'ordre sur un ensemble E. $A \subset E$. $M \in E$.*

(i) *M est un* majorant *de A si $\forall a \in A,\ a \lhd M$.*

(ii) *M est un* minorant *de A si $\forall a \in A,\ M \lhd a$.*

(iii) *M est un* plus grand élément *de A si $M \in A$ et majore A.*

(iv) *M est un* plus petit élément *de A si $M \in A$ et minore A.*

Proposition 3.45. *$\lhd$ une relation d'ordre sur un ensemble E. $A \subset E$. Si A admet un plus grand (ou plus petit) élément, alors cet élément est unique.*

Proposition 3.46. *$\lhd$ une relation d'ordre total sur un ensemble E. $A \subset E$. Si A est un sous-ensemble fini de E, alors A admet un plus petit et un plus grand élément.*

Démonstration. Par récurrence. □

Définition 3.47 (Élément maximal, minimal)**.** *$\lhd$ une relation d'ordre sur un ensemble E. $A \subset E, A \neq \varnothing$. $M \in E$.*

$$M \text{ est un élément maximal de } A \text{ si } \left\{ \begin{array}{l} M \in A \\ \forall a \in A,\ (M \lhd a \Rightarrow M = a) \end{array} \right. . \qquad \text{(i)}$$

$$M \text{ est un élément minimal de } A \text{ si } \left\{ \begin{array}{l} M \in A \\ \forall a \in A,\ (a \lhd M \Rightarrow a = M) \end{array} \right. . \qquad \text{(ii)}$$

Proposition 3.48. *$\lhd$ une relation d'ordre total sur un ensemble E. $A \subset E$.*

(i) *Si A admet un plus grand élément M, alors M est maximal.*

(ii) *Réciproquement, si A admet un élément maximal M, alors M est le plus grand élément de A.*

Définition 3.49. *$\lhd$ une relation d'ordre sur un ensemble E. $A \subset E, A \neq \varnothing$. $s \in E$.*

(i) *s est une* borne supérieur *de A, notée* $\sup A$*, si s est le plus petit des majorants de A.*

(ii) *s est une* borne inférieure *de A, notée* $\inf A$*, si s est le plus grand des minorants de A.*

Proposition 3.50. *Si A admet une borne supérieure (ou inférieure), alors elle est unique.*

Proposition 3.51. *$\lhd$ une relation d'ordre sur un ensemble E. $A \subset E, A \neq \varnothing$.*

(i) *Si A admet un plus grand élément M, alors $M = \sup A$.*

(ii) *Si A admet un plus petit élément m, alors $m = \inf A$.*

Proposition 3.52. *$A \subset \mathbb{R}, A \neq \varnothing$. $s \in \mathbb{R}$.*

$$s = \sup A \iff \begin{cases} s \text{ majore } A \\ \forall \varepsilon > 0,\ \exists a \in A,\ a > s - \varepsilon \end{cases}, \tag{i}$$

$$s = \inf A \iff \begin{cases} s \text{ minore } A \\ \forall \varepsilon > 0,\ \exists a \in A,\ a < s + \varepsilon \end{cases}. \tag{ii}$$

V.3 Relations d'équivalence

Définition 3.53 (Classe d'équivalence)**.** *$\mathcal{R}$ une relation d'équivalence sur un ensemble E non vide. $x \in E$. On appelle* classe d'équivalence *de x l'ensemble noté* $\mathrm{Cl}(x)$ *ou $\dot{x}$ et défini par*

$$\mathrm{Cl}(x) = \{y \in E,\ y \mathcal{R} x\}.$$

Proposition 3.54. *$\mathcal{R}$ une relation d'équivalence sur un ensemble E non vide. $(x, y) \in E^2$.*

$$\mathrm{Cl}(x) = \mathrm{Cl}(y) \iff x \mathcal{R} y.$$

Définition 3.55 (Partition)**.** *E, I des ensembles non vides. $(A_i)_{i \in I}$ une famille de parties de E. On dit que $(A_i)_{i \in I}$ est une* partition *de E lorsque les trois conditions suivantes sont vraies :*

$$\forall i \in I,\ A_i \neq \varnothing, \tag{i}$$

$$\bigcup_{i \in I} A_i = E, \tag{ii}$$

$$\forall (i, j) \in I^2,\ (A_i \cap A_j = \varnothing \text{ ou } A_i = A_j). \tag{iii}$$

Proposition 3.56. *$\mathcal{R}$ une relation d'équivalence sur un ensemble E non vide. Alors $(\mathrm{Cl}(x))_{x \in E}$ est une partition de E.*

Exemple 3.57 (Congruences)**.** *$(x, y) \in \mathbb{Z}^2$. $n \in \mathbb{N}^*$. On définit la congruence modulo n par $x \equiv y \quad [n] \iff n$ divise $(x - y)$. La relation de congruence modulo n possède n classes d'équivalence. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence modulo n.*

Chapitre 4

Introduction aux Systèmes Linéaires

Définition 4.1 (Système linéaire)**.** *On appelle* système linéaire *de n équations à p inconnues tout système de la forme suivante :*

$$(S):\begin{cases} a_{11}x_1 + \cdots + a_{1j}x_j + \cdots + a_{1p}x_p = b_1 \\ \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \\ a_{i1}x_1 + \cdots + a_{ij}x_j + \cdots + a_{ip}x_p = b_i \\ \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \\ a_{n1}x_1 + \cdots + a_{nj}x_j + \cdots + a_{np}x_p = b_n \end{cases}.$$

La matrice *du système est :*

$$\begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{ip} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{np} \end{pmatrix}.$$

Le second membre *du système est le vecteur* $(b_1, b_2, \ldots, b_n)$.

Vocabulaire 4.2. (i) *Un* système homogène *n'a pas de second membre.*

(ii) *Un* système compatible *admet au moins une solution.*

(iii) *Un* système de Cramer *admet exactement une solution.*

Proposition 4.3. *Soit (S) un système linéaire dont (S_0) est le système homogène associé. On appelle E l'ensemble des solutions de (S), E_0 l'ensemble des solutions de (S_0).*

$$X \in E \Longrightarrow E = \{X + X_0,\ X_0 \in E_0\}, \tag{i}$$

$$E_0 = \{0\} \text{ ou } E_0 \text{ est infini}, \tag{ii}$$

$$E = \varnothing \text{ ou } E \text{ est un singleton ou } E \text{ est infini}. \tag{iii}$$

Définition 4.4 (Système triangulaire)**.** *Un système de n équations à n inconnues est dit* triangulaire *lorsqu'il est du type :*

$$(S):\begin{cases} a_{11}x_1 + \cdots + a_{1i}x_i + \cdots + a_{1n}x_n = b_1 \\ \ddots \qquad\quad \vdots \qquad\quad \vdots \\ a_{ii}x_i + \cdots + a_{in}x_n = b_i \\ \qquad\quad \ddots \qquad\quad \vdots \\ a_{nn}x_n = b_n \end{cases}.$$

Proposition 4.5. *Un système triangulaire de n équations à n inconnues admet une unique solution* ssi $\forall i \in [\![1, n]\!]$, $a_{ii} \neq 0$.

Définition 4.6 (Opérations élémentaires)**.** *On appelle* opérations élémentaires *sur les lignes d'un système les opérations suivantes :*

(i) Transvection *:* $L_i \leftarrow L_i + \lambda L_j \quad (i \neq j)$.

(ii) Dilatation *:* $L_i \leftarrow \alpha L_i \quad (\alpha \neq 0)$.

(iii) Transposition *:* $L_i \leftrightarrow L_j$.

Des opérations élémentaires sur un système le transforment en un système équivalent.

Méthode 4.7 (Pivot de Gauss)**.** *En utilisant uniquement des opérations élémentaires sur des lignes ou des colonnes, on peut se ramener à un système triangulaire, que l'on sait résoudre.*

Chapitre 5

Fonctions Usuelles

I Généralités

Vocabulaire 5.1 (Fonction)**.** *Une application $f : D \subset \mathbb{R} \longrightarrow \mathbb{R}$, où $D \neq \varnothing$, est dite une* fonction *de $\mathbb{R}$ dans $\mathbb{R}$ définie sur D. Le* domaine de définition *de f est le plus grand ensemble sur lequel f est définie.*

Définition 5.2 (Parité, périodicité)**.** *$f : D \subset \mathbb{R} \to \mathbb{R}$ une fonction définie sur D. $T \in \mathbb{R}^*$.*

$$f \text{ est paire} \iff \forall x \in D,\ [(-x) \in D \text{ et } f(-x) = f(x)]. \tag{i}$$

$$f \text{ est impaire} \iff \forall x \in D,\ [(-x) \in D \text{ et } f(-x) = -f(x)]. \tag{ii}$$

$$f \text{ est } T\text{-périodique} \iff \forall x \in D,\ [(x+T) \in D \text{ et } f(x+T) = f(x)]. \tag{iii}$$

Proposition 5.3. *$f : D \subset \mathbb{R} \to \mathbb{R}$ une fonction. $(a, b) \in \mathbb{R}^2$. $\mathscr{C}_f$ le graphe de f.*

(i) *Supposons que $\forall x \in D$, $[(a-x) \in D$ et $f(a-x) = f(x)]$. Alors $\mathscr{C}_f$ est symétrique par rapport à la droite $x = \frac{a}{2}$.*

(ii) *Supposons que $\forall x \in D$, $[(a-x) \in D$ et $f(a-x) = b - f(x)]$. Alors $\mathscr{C}_f$ est symétrique par rapport au point $\left(\frac{a}{2}, \frac{b}{2}\right)$.*

(iii) *Supposons que f est T-périodique. Alors $\mathscr{C}_f$ est invariant par translation par le vecteur $(T, 0)$.*

Vocabulaire 5.4 (Affinité)**.** *On appelle* affinité *de rapport λ, de base (Ox) (resp. (Oy)) et de direction (Oy) (resp. (Ox)) l'application $M(x, y) \longmapsto M'(x, \lambda y)$ (resp. $M(x, y) \longmapsto M'(\lambda x, y)$).*

Proposition 5.5. *$f : D \subset \mathbb{R} \to \mathbb{R}$ une fonction bijective.*

$$\mathscr{C}_f \text{ et } \mathscr{C}_{f^{-1}} \text{ sont symétriques par rapport à la droite } y = x. \tag{i}$$

$$\text{Si } f \nearrow \text{ sur } D \text{ alors } f^{-1} \nearrow \text{ sur } f(D). \tag{ii}$$

$$\text{Si } f \searrow \text{ sur } D \text{ alors } f^{-1} \searrow \text{ sur } f(D). \tag{iii}$$

Définition 5.6 (Majorant, minorant)**.** *$f : D \subset \mathbb{R} \to \mathbb{R}$ une fonction. On dit que M* majore *(resp.* minore*) f sur D lorsque $\forall x \in D$, $f(x) \leqslant M$ (resp. $f(x) \geqslant M$).*

Définition 5.7 (Extremum global)**.** *$f : D \subset \mathbb{R} \to \mathbb{R}$ une fonction. On dit que $f(x_0)$ est un* maximum global *(resp.* minimum global*) sur D lorsque $\forall x \in D$, $f(x) \leqslant f(x_0)$ (resp. $f(x) \geqslant f(x_0)$).*

Définition 5.8 (Extremum local)**.** *$f : D \subset \mathbb{R} \to \mathbb{R}$ une fonction. On dit que $f(x_0)$ est un* maximum local *(resp.* minimum local*) sur D lorsqu'il existe un $\alpha \in \mathbb{R}_+^*$ t.q. $f_{|(]x_0-\alpha,x_0+\alpha[\cap D)}$ admet $f(x_0)$ comme maximum global (resp. minimum global).*

Définition 5.9 (Asymptotes)**.** *$f : D \subset \mathbb{R} \to \mathbb{R}$ une fonction. $x_0 \in \mathbb{R}$. $\mathscr{C}_f$ le graphe de f.*

(i) $\lim_{x\to x_0} f(x) = \pm\infty$ ssi *la droite $x = x_0$ est une asymptote verticale à $\mathscr{C}_f$.*

(ii) $\lim_{x\to\pm\infty} |f(x) - (ax + b)| = 0$ ssi *la droite $y = ax + b$ est une asymptote à $\mathscr{C}_f$.*

II Valeur absolue, partie entière, etc.

II.1 Valeur absolue

Définition 5.10 (Valeur absolue)**.**

$$\left|\begin{array}{l} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto \left\{ \begin{array}{ll} x & si\ x \geqslant 0 \\ -x & sinon \end{array} \right. \end{array}\right. .$$

Proposition 5.11.

$$\forall (x, y) \in \mathbb{R}^2,\ |xy| = |x||y|, \tag{i}$$

$$\forall (x, y) \in \mathbb{R}^2,\ |x + y| \leqslant |x| + |y|, \tag{ii}$$

$$\forall (x, a) \in \mathbb{R}^2,\ \forall r \in \mathbb{R}_+^*,\ (|x - a| \leqslant r \iff x \in [a - r, a + r]), \tag{iii}$$

$$\forall (x, y) \in \mathbb{R}^2,\ \max(x, y) = \frac{x + y + |x - y|}{2}, \tag{iv}$$

$$\forall (x, y) \in \mathbb{R}^2,\ \min(x, y) = \frac{x + y - |x - y|}{2}, \tag{v}$$

$$\forall x \in \mathbb{R},\ \sqrt{x^2} = |x|. \tag{vi}$$

II.2 Partie entière

Définition 5.12 (Partie entière, partie fractionnaire)**.** *$x \in \mathbb{R}$.*

$$\lfloor x \rfloor \text{ est le plus grand entier inférieur ou égal à } x. \tag{i}$$

$$\lceil x \rceil \text{ est le plus petit entier supérieur ou égal à } x. \tag{ii}$$

$$\{x\} \text{ est défini par } \{x\} = x - \lfloor x \rfloor. \tag{iii}$$

Proposition 5.13. $\forall x \in \mathbb{R},\ \forall k \in \mathbb{Z},\ \lfloor x + k \rfloor = \lfloor x \rfloor + k$.

III Continuité

Définition 5.14 (Continuité). *I, J des intervalles (non vides et non réduits à un point). $f : I \to \mathbb{R}$. $a \in I \cup \{\inf I, \sup I\}$. On dit que f est* continue *(ou $\mathcal{C}^0$) en a lorsque $\lim_{x\to a} f(x)$ existe et est réelle.*

Définition 5.15 (Prolongement par continuité). *Si a est une borne de I, $a \notin I$ mais f continue en a, alors f est* prolongeable par continuité *en a et son prolongement est :*

$$\begin{vmatrix} I \cup \{a\} \longrightarrow \mathbb{R} \\ x \longmapsto \begin{cases} f(x) & si\ x \neq a \\ \lim_{x\to a} f(x) & sinon \end{cases} \end{vmatrix} .$$

Théorème 5.16 (Théorème des valeurs intermédiaires). *$f : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I.*

$$\forall (a,b) \in I^2,\ \forall \gamma \in [f(a), f(b)],\ \exists c \in [a,b],\ \gamma = f(c).$$

Théorème 5.17 (Théorème de la bijection). *I un intervalle. $f : I \to \mathbb{R}$ $\mathcal{C}^0$ et strictement monotone sur I. Alors $\widetilde{f} : \begin{vmatrix} I \to f(I) \\ x \longmapsto f(x) \end{vmatrix}$ est une bijection et $\widetilde{f}^{-1}$ est $\mathcal{C}^0$ sur $f(I)$.*

Proposition 5.18. *I un intervalle. $f : I \to \mathbb{R}$ $\mathcal{C}^0$ et strictement monotone sur I. Alors*

$$\lim_{x\to+\infty} f(x) = \ell \Longrightarrow \lim_{x\to\ell} f^{-1}(x) = +\infty, \quad avec\ \ell \in \mathbb{R} \cup \{\pm\infty\}.$$

IV Dérivabilité

Définition 5.19 (Dérivabilité). *$f : I \to \mathbb{R}$. $a \in I \cup \{\inf I, \sup I\}$. Pour $t \in I$, on note $\tau_a(t) = \frac{f(t)-f(a)}{t-a}$. On dit que f est* dérivable *en a lorsque $\lim_{t\to a} \tau_a(t)$ existe et est réelle. Si f est dérivable en tout point de I, on définit*

$$f' : \begin{vmatrix} I \longrightarrow \mathbb{R} \\ x \longmapsto \lim\limits_{t\to x} \tau_x(t) \end{vmatrix} .$$

Définition 5.20 (Dérivabilité à droite, à gauche). *f est dérivable en a à droite (resp. à gauche) lorsque $\lim_{t\to a^+} \tau_a(t)$ (resp. $\lim_{t\to a^-} \tau_a(t)$) existe et est réelle.*

Définition 5.21 (Tangente). *$f : I \to \mathbb{R}$ dérivable en $\alpha \in I$. On appelle* tangente *à $\mathscr{C}_f$ en α la droite d'équation*

$$y = f(\alpha) + (x - \alpha) f'(\alpha).$$

Définition 5.22 (Dérivée n-ième). *$f : I \to \mathbb{R}$. $n \in \mathbb{N}$. On définit $f^{(n)}$ par :*

$$\begin{cases} f^{(0)} = f \\ \forall n \in \mathbb{N},\ f^{(n)}\ dérivable\ sur\ I \Longrightarrow f^{(n+1)} = \left(f^{(n)}\right)' \end{cases} .$$

On dit que f est n fois dérivable sur I lorsque $f^{(n)}$ est définie sur I.

Définition 5.23 ($\mathcal{C}^n$). *$f : I \to \mathbb{R}$. $n \in \mathbb{N}$. On dit que f est de classe $\mathcal{C}^n$ lorsque f est n fois dérivable sur I et $f^{(n)}$ est $\mathcal{C}^0$ sur I.*

Notation 5.24 ($\mathcal{C}^n$)**.** *$f : I \to \mathbb{R}$. On dit que f est $\mathcal{C}^\infty$ lorsque $\forall n \in \mathbb{N}$, f $\mathcal{C}^n$.*

Proposition 5.25. *$f : I \to \mathbb{R}$. $n \in \mathbb{N}^*$.*

$$f \ \mathcal{C}^n \text{ sur } I \iff f \text{ dérivable sur } I \text{ et } f' \ \mathcal{C}^{n-1} \text{ sur } I.$$

Proposition 5.26. *f, g $\mathcal{C}^n$ sur I. $\lambda \in \mathbb{R}$. Les fonctions $(f+g), (fg), (\lambda f), \left(\frac{1}{g}\right)$ (si g ne s'annule pas) sont $\mathcal{C}^n$ sur I.*

Proposition 5.27. *$f : I \to \mathbb{R}$ $\mathcal{C}^n$ sur I, $g : J \to \mathbb{R}$ $\mathcal{C}^n$ sur J, avec $f(I) \subset J$. Alors $(g \circ f)$ $\mathcal{C}^n$ sur I.*

Théorème 5.28 (Formule de Leibniz)**.** *f, g $\mathcal{C}^n$ sur I. Alors*

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}.$$

V Ordre et dérivée

Proposition 5.29. *$f : I \to \mathbb{R}$ dérivable sur I.*

$$f' \geqslant 0 \text{ sur } I \iff f \nearrow \text{ sur } I \qquad \text{et} \qquad f' \leqslant 0 \text{ sur } I \iff f \searrow \text{ sur } I. \tag{i}$$

$$f' = 0 \text{ sur } I \iff f \text{ constante sur } I. \tag{ii}$$

$$f' > 0 \text{ sur } I \implies f \nearrow\nearrow \text{ sur } I \qquad \text{et} \qquad f' < 0 \text{ sur } I \implies f \searrow\searrow \text{ sur } I. \tag{iii}$$

Proposition 5.30. *$f : I \to \mathbb{R}$ dérivable sur I. Si $f' > 0$ (resp. < 0) sur I excepté en un nombre fini de points où $f' = 0$, alors $f \nearrow\nearrow$ (resp. $f \searrow\searrow$) sur I.*

Proposition 5.31. *$f : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I intervalle. $a \in I \cap \{\inf I, \sup I\}$. Si f dérivable sur $I \backslash \{a\}$ et $f' > 0$ sur $I \backslash \{a\}$ alors $f \nearrow\nearrow$ sur I.*

Proposition 5.32. *$f : I \to \mathbb{R}$ définie sur I intervalle, $a \in I \backslash \{\inf I, \sup I\}$. On suppose que f est dérivable en a et que $f(a)$ est un extremum local. Alors $f'(a) = 0$.*

Définition 5.33 (Fonction convexe, concave)**.** *$f : I \to \mathbb{R}$ définie sur I intervalle. f est dite* convexe *sur I lorsque le graphe de f est en-dessous de chacune de ses cordes, i.e.*

$$\forall (a,b) \in I^2, \ \forall \lambda \in [0,1], \ \underbrace{\lambda f(a) + (1-\lambda) f(b)}_{\text{Point sur la corde}} \geqslant \underbrace{f(\lambda a + (1-\lambda) b)}_{\text{Point sur le graphe}}.$$

f est dite concave *lorsque $(-f)$ est convexe.*

Proposition 5.34. *$f : I \to \mathbb{R}$ définie et dérivable sur I intervalle. Si $f' \nearrow$ sur I, alors*

(i) *f est convexe sur I.*

(ii) *$\mathscr{C}_f$ est au-dessus de chacune de ses tangentes.*

Démonstration. (i) Fixer $(a,b) \in I^2, a \leqslant b$ et étudier $\varphi : \lambda \in [0,1] \longmapsto \lambda f(a) + (1-\lambda) f(b) - f(\lambda a + (1-\lambda) b)$. (ii) Fixer $a \in I$ et étudier $\psi : x \in \mathbb{R} \longmapsto f(x) - f(a) - (x-a) f'(a)$. □

VI Application réciproque

Proposition 5.35. *$f : I \to \mathbb{R}$ définie et dérivable (resp. $\mathcal{C}^n$, $\mathcal{C}^\infty$) sur I intervalle. On suppose f bijective de I sur $f(I)$, f' ne s'annule pas sur I. Alors f^{-1} dérivable (resp. $\mathcal{C}^n$, $\mathcal{C}^\infty$) sur $f(I)$ et*

$$\left(f^{-1}\right)' = \frac{1}{f' \circ f^{-1}}.$$

VII Dérivabilité de $f : I \subset \mathbb{R} \to \mathbb{C}$

Définition 5.36 (Limites dans $\mathbb{C}$)**.** *$f : I \subset \mathbb{R} \to \mathbb{C}$. Soit $a \in I$. On dit que f admet une* limite $\ell \in \mathbb{C}$ *lorsque $|f(x) - \ell| \xrightarrow[x\to a]{} 0$.*

Proposition 5.37. *$f : I \subset \mathbb{R} \to \mathbb{C}$. $a \in I$. $\ell \in \mathbb{C}$.*

$$f(x) \xrightarrow[x\to a]{} \ell \iff \begin{cases} \Re(f(x)) \xrightarrow[x\to a]{} \Re(\ell) \\ \Im(f(x)) \xrightarrow[x\to a]{} \Im(\ell) \end{cases}.$$

Définition 5.38 (Continuité dans $\mathbb{C}$)**.** *$f : I \subset \mathbb{R} \to \mathbb{C}$. $a \in I \cup \{\inf I, \sup I\}$. f est dite* continue *en a lorsque f admet une limite finie en a.*

Définition 5.39 (Dérivabilité dans $\mathbb{C}$)**.** *$f : I \subset \mathbb{R} \to \mathbb{C}$. $a \in I \cup \{\inf I, \sup I\}$. f est dite* dérivable *en a lorsque $\tau_a(t)$ (c.f. définition 5.19) admet une limite finie en a.*

Proposition 5.40. *$f : I \subset \mathbb{R} \to \mathbb{C}$. f est dérivable (resp. $\mathcal{C}^n$, $\mathcal{C}^\infty$) sur I* ssi *$\Re(f)$ et $\Im(f)$ le sont toutes deux, et on a :*

$$f' = [\Re(f)]' + i[\Im(f)]'.$$

Proposition 5.41. *Soit $f : I \subset \mathbb{R} \to \mathbb{C}$ dérivable (resp. $\mathcal{C}^n$, $\mathcal{C}^\infty$) sur I. Alors $(\exp \circ f) : I \to \mathbb{C}$ est dérivable (resp. $\mathcal{C}^n$, $\mathcal{C}^\infty$) sur I et*

$$(\exp \circ f)' = f' \cdot (\exp \circ f).$$

VIII Logarithme, exponentielle, arc sinus, etc.

VIII.1 Rappels

Définition 5.42 (Primitive)**.** *Soit $f : I \to \mathbb{R}$. Alors $F : I \to \mathbb{R}$ est une primitive de f lorsque F est dérivable sur I et que $F' = f$.*

Proposition 5.43. *Toutes les primitives d'une fonction, s'il en existe, diffèrent d'une constante.*

Proposition 5.44. *$f, g : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I intervalle. $a \in I$. F, G primitives de f, g.*

(i) *f admet une primitive sur I.*

(ii) *f admet sur I une unique primitive qui s'annule en a.*

(iii) *Si $f \leqslant g$ alors $F \leqslant G$ sur $I \cap [a, +\infty[$.*

Théorème 5.45 (Théorème de la limite monotone)**.** *I un intervalle de la forme $[a, b[$ où $b \in \mathbb{R} \cup \{+\infty\}$. $f : I \to \mathbb{R}$. On suppose que $f \nearrow$, $\mathcal{C}^0$ sur I. On a l'alternative suivante :*

$$f \text{ majorée sur } I \implies \exists \ell \in \mathbb{R},\ f(x) \xrightarrow[x\to b]{} \ell. \tag{i}$$

$$f \text{ non majorée sur } I \implies f(x) \xrightarrow[x\to b]{} +\infty. \tag{ii}$$

VIII.2 Logarithme

Définition 5.46 (Logarithme népérien)**.** ln *est l'unique primitive de* $x \mapsto \frac{1}{x}$ *sur* $\mathbb{R}_+^*$ *qui s'annule en* 1*.*

Proposition 5.47.

$$\ln \text{ est } \mathcal{C}^\infty, \nearrow\nearrow \text{ sur } \mathbb{R}_+^*. \tag{i}$$

$$\forall (a,b) \in \left(\mathbb{R}_+^*\right)^2, \forall n \in \mathbb{Z}, \begin{cases} \ln(ab) = \ln a + \ln b \\ \ln\left(\frac{a}{b}\right) = \ln a - \ln b \\ \ln\left(a^n\right) = n \ln a \end{cases}. \tag{ii}$$

$$\ln \text{ est concave sur } \mathbb{R}_+^*. \tag{iii}$$

$$\forall x \in \mathbb{R}_+^*, \ln x \leqslant x - 1. \tag{iv}$$

$$\ln x \xrightarrow[x\to+\infty]{} +\infty \quad et \quad \ln x \xrightarrow[x\to 0^+]{} -\infty \quad et \quad \frac{\ln(1+x)}{x} \xrightarrow[x\to 0]{} 1. \tag{v}$$

Proposition 5.48. $f : I \to \mathbb{R}^*$ *dérivable sur* I*. Alors* $(\ln|f|)' = \frac{f'}{f}$*.*

Notation 5.49. *On note* e *l'unique élément de* $\mathbb{R}_+^*$ *t.q.* $\ln e = 1$*.*

VIII.3 Exponentielle

Définition 5.50 (Exponentielle)**.** exp *est la fonction réciproque de* ln *(qui est une bijection de* $\mathbb{R}_+^*$ *sur* $\mathbb{R}$*).*

Proposition 5.51.

$$\exp \text{ est } \mathcal{C}^\infty, \nearrow\nearrow \text{ sur } \mathbb{R} \text{ et } \exp' = \exp, \exp(0) = 1. \tag{i}$$

$$\forall (a,b) \in \mathbb{R}^2, \forall n \in \mathbb{Z}, \begin{cases} \exp(a+b) = \exp a \cdot \exp b \\ \exp(a-b) = \frac{\exp a}{\exp b} \\ \exp(na) = (\exp a)^n \end{cases}. \tag{ii}$$

$$\exp \text{ est convexe sur } \mathbb{R}. \tag{iii}$$

$$\forall x \in \mathbb{R}, \exp x \geqslant x + 1. \tag{iv}$$

$$\exp x \xrightarrow[x\to+\infty]{} +\infty \quad et \quad \exp x \xrightarrow[x\to-\infty]{} 0 \quad et \quad \frac{\exp x - 1}{x} \xrightarrow[x\to 0]{} 1. \tag{v}$$

VIII.4 Fonctions puissances

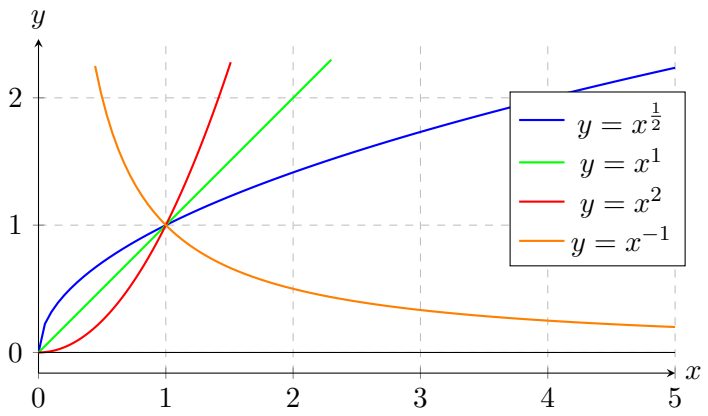
Définition 5.52 (Fonctions puissances)**.** $\alpha \in \mathbb{R}$*. La fonction puissance* α *est définie par*

$$f_\alpha : \left| \begin{array}{l} \mathbb{R}_+^* \longrightarrow \mathbb{R} \\ x \longmapsto \exp(\alpha \ln x) \end{array} \right. .$$

On notera $x^\alpha = f_\alpha(x)$*.*

Proposition 5.53. $(\alpha, \beta) \in \mathbb{R}^2$*.* $(x,y) \in \left(\mathbb{R}_+^*\right)^2$*. Alors* $\ln(x^\alpha) = \alpha \ln x$*,* $x^\alpha y^\alpha = (xy)^\alpha$*,* $\left(x^\alpha\right)^\beta = x^{\alpha\beta}$ *et* $x^\alpha x^\beta = x^{\alpha+\beta}$*.*

Proposition 5.54. *Pour* $\alpha \in \mathbb{R}^*$*,* f_α *réalise une bijection de* $\mathbb{R}_+^*$ *sur* $\mathbb{R}_+^*$ *et* $f_\alpha^{-1} = f_{\frac{1}{\alpha}}$*.*



VIII.5 Croissances comparées

Proposition 5.55. $(a, b) \in \left(\mathbb{R}_+^*\right)^2$.

$$\frac{(\ln x)^b}{x^a} \xrightarrow[x\to+\infty]{} 0^+ \qquad et \qquad x^a |\ln x|^b \xrightarrow[x\to 0^+]{} 0^+.$$

Démonstration. Utiliser $\frac{1}{x} < \frac{1}{\sqrt{x}}$ (pour $x > 1$) et en déduire que $x \mapsto 2\sqrt{x} - \ln x$ est $\nearrow\nearrow$, ce qui implique $2\sqrt{x} - \ln x > 2$, d'où $\frac{\ln x}{x} < \frac{2\sqrt{x}-2}{x} \xrightarrow[x\to+\infty]{} 0$. En déduire enfin que $\frac{(\ln x)^b}{x^a} \xrightarrow[x\to+\infty]{} 0^+$. □

Corollaire 5.56. $(a, b) \in \left(\mathbb{R}_+^*\right)^2$.

$$\frac{e^{ax}}{x^b} \xrightarrow[x\to+\infty]{} +\infty \qquad et \qquad |x|^b e^{ax} \xrightarrow[x\to-\infty]{} 0^+.$$

Proposition 5.57. *Soit u dérivable sur I intervalle, $u > 0$ sur I. $\alpha \in \mathbb{R}$. Alors $u^\alpha = f_\alpha \circ u$ est dérivable sur I et*

$$(u^\alpha)' = \alpha u' u^{\alpha-1}.$$

VIII.6 Fonctions hyperboliques

Définition 5.58 (Sinus, cosinus et tangente hyperboliques)**.**

$$\mathrm{sh} : x \in \mathbb{R} \longmapsto \frac{e^x - e^{-x}}{2} \qquad et \qquad \mathrm{ch} : x \in \mathbb{R} \longmapsto \frac{e^x + e^{-x}}{2},$$

$$\mathrm{th} : x \in \mathbb{R} \longmapsto \frac{\mathrm{sh}(x)}{\mathrm{ch}(x)}.$$

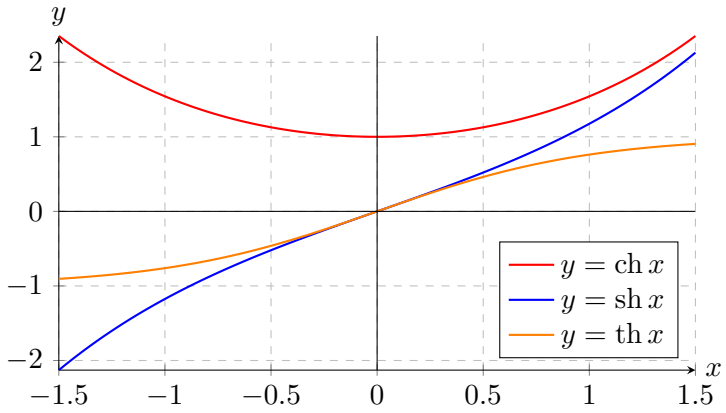
Proposition 5.59. $x \in \mathbb{R}$.

$$\mathrm{ch}\, x + \mathrm{sh}\, x = e^x \qquad et \qquad \mathrm{ch}^2 x - \mathrm{sh}^2 x = 1, \tag{i}$$

$$\mathrm{ch}' = \mathrm{sh} \quad et \quad \mathrm{sh}' = \mathrm{ch} \quad et \quad \mathrm{th}' = 1 - \mathrm{th}^2 = \frac{1}{\mathrm{ch}^2}, \tag{ii}$$

$$\mathrm{sh}(2x) = 2\,\mathrm{sh}\, x\, \mathrm{ch}\, x, \tag{iii}$$

$$\mathrm{ch}(2x) = \mathrm{ch}^2 x + \mathrm{sh}^2 x = 1 + 2\,\mathrm{sh}^2 x. \tag{iv}$$



VIII.7 Fonctions trigonométriques inverses

Proposition 5.60. $x \in [0, \frac{\pi}{2}[$.

$$\frac{2}{\pi}x \leqslant \sin x \leqslant x \leqslant \tan x.$$

Définition 5.61 (Arc sinus, arc cosinus, arc tangente)**.** *Les applications* $\sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$, $\cos : [0, \pi] \to [-1, 1]$ *et* $\tan :]-\frac{\pi}{2}, \frac{\pi}{2}[\to \mathbb{R}$ *sont bijectives. On note* arcsin, arccos *et* arctan *leurs fonctions réciproques respectives.*

Proposition 5.62.

$$\forall x \in [-1, 1],\ \arccos x + \arcsin x = \frac{\pi}{2}, \tag{i}$$

$$\forall x \in \mathbb{R}^*,\ \arctan x + \arctan \frac{1}{x} = \begin{cases} \frac{\pi}{2} & si\ x > 0 \\ -\frac{\pi}{2} & si\ x < 0 \end{cases}, \tag{ii}$$

$$\forall x \in [-1, 1],\ \sin(\arccos x) = \cos(\arcsin x) = \sqrt{1 - x^2}. \tag{iii}$$

Proposition 5.63. arcsin *et* arccos *sont* $\mathcal{C}^\infty$ *sur* $]-1, 1[$, arctan $\mathcal{C}^\infty$ *sur* $\mathbb{R}$.

$$\forall x \in]-1, 1[,\ \arcsin' x = \frac{1}{\sqrt{1 - x^2}}, \tag{i}$$

$$\forall x \in]-1, 1[,\ \arccos' x = -\frac{1}{\sqrt{1 - x^2}}, \tag{ii}$$

$$\forall x \in \mathbb{R},\ \arctan' x = \frac{1}{1 + x^2}. \tag{iii}$$

Chapitre 6

Équations Différentielles Linéaires

Vocabulaire 6.1. *Soit $F : I \times \mathbb{K}^p \to \mathbb{K}$. Résoudre l'équation différentielle $y^{(p)} = F(t, y, y', \dots, y^{(p-1)})$ sur un intervalle I, c'est déterminer toutes les fonctions $y : I \to \mathbb{K}$ p fois dérivables sur I t.q.*

$$\forall t \in I,\ y^{(p)}(t) = F(t, y(t), y'(t), \dots, y^{(p-1)}(t)).$$

I Généralités

Définition 6.2 (Équation différentielle linéaire)**.** *Une* équation différentielle linéaire *d'ordre N est une équation du type*

$$\sum_{k=0}^{N} a_k y^{(k)} = c, \qquad (E_c)$$

sur un intervalle $I \subset \mathbb{R}$, où $a_0, \dots, a_N : I \to \mathbb{K}$, $a_N \neq 0$ et $c : I \to \mathbb{K}$.

Proposition 6.3. *Soit y_p une* solution particulière *de (E_c). On appelle (E_0) l'équation de second membre nul, dite* équation homogène*. Alors l'ensemble $\mathcal{S}$ des solutions de (E_c) est*

$$\mathcal{S} = \{y_p + y_h,\ y_h \text{ solution de } (E_0)\}.$$

Définition 6.4 (Courbe intégrale)**.** *On appelle* courbe intégrale *de (E_c) toute courbe représentative d'une solution de (E_c).*

Proposition 6.5. *Soit $c, d : I \to \mathbb{K}$, $\mathcal{S}_u$ l'ensemble des solutions de (E_u).*

$$\left.\begin{array}{l}(y : I \to \mathbb{K}) \in \mathcal{S}_c \\ (z : I \to \mathbb{K}) \in \mathcal{S}_d\end{array}\right\} \Longrightarrow \forall (\lambda, \mu) \in \mathbb{K}^2,\ (\lambda y + \mu z) \in \mathcal{S}_{\lambda c + \mu d}. \qquad \text{(i)}$$

$$a_0, \dots, a_N \text{ à valeurs dans } \mathbb{R} \Longrightarrow (y \in \mathcal{S}_c \Leftrightarrow \overline{y} \in \mathcal{S}_{\overline{c}})\,. \qquad \text{(ii)}$$

II Conditions initiales

Définition 6.6 (Problème de Cauchy)**.** *On dit que l'on résout un* problème de Cauchy *en $a \in I$ lorsque l'on cherche les solutions de (E_c) vérifiant*

$$(y(a), y'(a), \dots, y^{(N-1)}(a)) = (\alpha_0, \alpha_1, \dots, \alpha_{N-1}),$$

où $(\alpha_0, \alpha_1, \dots, \alpha_{N-1}) \in \mathbb{K}^N$ donné.

III Équations différentielles linéaires du premier ordre

Proposition 6.7 (Solutions de l'équation homogène)**.** *Soit $a : I \to \mathbb{K}$ $\mathcal{C}^0$ sur I intervalle. Alors les solutions de l'équation $y' + ay = 0$ sur I sont les*

$$y : t \in I \longmapsto \lambda e^{-A(t)},$$

où A est une primitive fixée de a sur I, et $\lambda \in \mathbb{K}$.

Démonstration. Supposer que y est solution de l'équation homogène et poser $z = y \cdot (\exp \circ A)$. Montrer alors que $z' = 0$ sur I et en déduire que z est constante. □

Proposition 6.8 (Solution particulière)**.** *Supposons $a, b : I \to \mathbb{K}$ $\mathcal{C}^0$ sur I intervalle. Alors l'équation $y' + ay = b$ sur I admet une solution particulière.*

Démonstration. Chercher une solution particulière y_p sous la forme $y_p = c \cdot (\exp \circ(-A))$, où $c : I \to \mathbb{K}$ est une fonction dérivable à déterminer. Montrer que y_p solution de l'équation ssi $c' = b \cdot (\exp \circ A)$, et en déduire que $y_p = c \cdot (\exp \circ(-A))$ convient. □

Proposition 6.9 (Solution du problème de Cauchy)**.** *Soit $a, b : I \to \mathbb{K}$ $\mathcal{C}^0$ sur I intervalle. $t_0 \in I, y_0 \in \mathbb{K}$. Alors le problème de Cauchy*

$$\begin{cases} y' + ay = b \\ y(t_0) = y_0 \end{cases}$$

admet une unique solution sur I.

Remarque 6.10. *Si a est une fonction constante et b est de la forme $t \in \mathbb{R} \mapsto e^{mt} \cdot P(t)$, où P est une fonction polynomiale et $m \in \mathbb{K}$, alors on peut chercher y_p sous la forme $t \in \mathbb{R} \mapsto e^{mt} \cdot Q(t)$, où Q est une fonction polynomiale. Pour cela, il faut dériver y_p puis résoudre $Q'(t) + (a + m)Q(t) = P(t)$.*

IV Équations différentielles linéaires du deuxième ordre à coefficients constants

Définition 6.11 (Équation caractéristique)**.** *$(a, b) \in \mathbb{K}^2$. On appelle* équation caractéristique *de l'équation $y'' + ay' + by = 0$ l'équation $r^2 + ar + b = 0$, où $r \in \mathbb{K}$.*

Proposition 6.12 (Solutions de l'équation homogène)**.** *$(a, b) \in \mathbb{K}^2$. L'ensemble $\mathcal{S}$ des solutions de $y'' + ay' + by = 0$ sur I intervalle est :*

$$\mathcal{S} = \{\lambda u + \mu v,\ (\lambda, \mu) \in \mathbb{K}^2\},$$

où $u : I \to \mathbb{K}$ et $v : I \to \mathbb{K}$ sont définies ci-dessous (on note Δ le discriminant, r_1, r_2 les racines de l'équation caractéristique $r^2 + ar + b = 0$) :

	$\Delta \in \mathbb{R}_+$	$\Delta = 0$	$\Delta \in \mathbb{C}\backslash\mathbb{R}_+$
$\mathbb{K} = \mathbb{C}$	$u : t \longmapsto e^{r_1 t}$ $v : t \longmapsto e^{r_2 t}$	$u : t \longmapsto e^{r_1 t}$ $v : t \longmapsto te^{r_1 t}$	$u : t \longmapsto e^{r_1 t}$ $v : t \longmapsto e^{r_2 t}$
$\mathbb{K} = \mathbb{R}$			$u : t \longmapsto e^{\alpha t}\cos(\beta t)$ $v : t \longmapsto e^{\alpha t}\sin(\beta t)$

avec $\alpha = \Re(r_1), \beta = \Im(r_1)$.

Démonstration. Supposer que y est solution de l'équation homogène et poser $z : t \mapsto y(t)e^{-rt}$, avec r racine de l'équation caractéristique. Montrer alors que z' vérifie $z'' + (2r + a)z' = 0$, et en déduire que $\exists \lambda \in \mathbb{K}, \forall t \in I, z'(t) = \lambda e^{-(2r+a)t}$. Discuter selon que $2r+a = 0$ ou non (ce qui équivaut à $\Delta = 0$) et selon que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$. □

Proposition 6.13 (Solution particulière)**.** *$(a, b) \in \mathbb{K}^2$. $c : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I intervalle. Alors l'équation $y'' + ay' + by = c$ admet une solution particulière sur I.*

Proposition 6.14 (Solution du problème de Cauchy)**.** *$(a, b) \in \mathbb{K}^2$. $c : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I intervalle. $t_0 \in I, (\alpha, \beta) \in \mathbb{K}^2$. Alors le problème de Cauchy*

$$\begin{cases} y'' + ay' + by = c \\ y(t_0) = \alpha \\ y'(t_0) = \beta \end{cases}$$

admet une unique solution sur I.

Remarque 6.15. *Quelques cas particuliers où l'on sait calculer une solution particulière :*

(i) *$b \neq 0$ et c est une fonction constante. Alors $y'' + ay' + by = c$ a pour solution $\frac{c}{b}$.*

(ii) *c est de la forme $c : t \mapsto \gamma e^{mt}$. Alors $y'' + ay' + by = c$ a une solution de la forme $t \mapsto \lambda t^k e^{mt}$, avec $k \in \{0, 1, 2\}$.*

(iii) *c est de la forme $c : t \mapsto \cos(\omega t)$ (ou $\sin(\omega t)$). Alors on se ramène au cas précédent avec $\gamma = 1, m = i\omega$.*

Chapitre 7

Calculs de Primitives

I Généralités

Définition 7.1 (Intégrale)**.** *Soit* $(a,b) \in \mathbb{R}^2$, $f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0$ *sur* $[a,b]$. *On note* $\int_a^b f$ *l'aire algébrique entre* $\mathscr{C}_f$ *et* (Ox).

Théorème 7.2. $f : I \to \mathbb{R}$ $\mathcal{C}^0$ *sur* I *intervalle.* $\alpha \in I$. *Alors :*

(i) f *admet une primitive sur* I.

(ii) $x \in I \longmapsto \int_\alpha^x f$ *est l'unique primitive de* f *qui s'annule en* α.

Proposition 7.3. $f, g : I \to \mathbb{R}$ $\mathcal{C}^0$ *sur* I *intervalle.* $(a,b) \in I^2$. F *une primitive de* f *sur* I. *Alors :*

(i) $(f \leqslant g$ *sur* I et $a \leqslant b) \Longrightarrow \int_a^b f \leqslant \int_a^b g$.

(ii) $\left(f \geqslant 0$ *sur* I et $\int_a^b f = 0\right) \Longrightarrow f = 0$ *sur* I.

Proposition 7.4. $f : I \to \mathbb{C}$ $\mathcal{C}^0$ *sur* I *intervalle.*

(i) f *admet une primitive sur* I.

(ii) F *primitive de* f *sur* $I \iff \begin{cases} \Re(F) \text{ primitive de } \Re(f) \text{ sur } I \\ \Im(F) \text{ primitive de } \Im(f) \text{ sur } I \end{cases}$.

Définition 7.5 (Intégrale d'une fonction à valeurs dans $\mathbb{C}$)**.** $f : I \to \mathbb{C}$ $\mathcal{C}^0$ *sur* I *intervalle.* $(a,b) \in I^2$. *Alors on définit*

$$\int_a^b f = \int_a^b \Re(f) + i \int_a^b \Im(f).$$

Proposition 7.6. $f : I \to \mathbb{K}$ $\mathcal{C}^0$ *sur* I *intervalle.* $(a,b) \in I^2$. F *une primitive de* f *sur* I. *Alors*

$$\int_a^b f = F(b) - F(a).$$

II Intégration par parties

Proposition 7.7 (Intégration par parties)**.** $u, v : I \to \mathbb{K}$ $\mathcal{C}^1$ *sur* I *intervalle.* $(a,b) \in I^2$. *Alors*

$$\int_a^b u'v = [uv]_a^b - \int_a^b uv'.$$

Corollaire 7.8. *Pour $k \in \mathbb{N}$, les primitives de $x \mapsto x^k e^x$ sont du type $x \mapsto P(x)e^x$, où P est une fonction polynomiale de degré k.*

Démonstration. Par récurrence. □

III Intégration par substitution

Proposition 7.9 (Intégration par substitution)**.** *$f : I \to \mathbb{K}$ $\mathcal{C}^0$ sur I intervalle. $\varphi : J \to \mathbb{K}$ $\mathcal{C}^1$ sur J avec $\varphi(J) \subset I$. $(\alpha, \beta) \in J^2$.*

$$\int_{\varphi(\alpha)}^{\varphi(\beta)} f(x)\ \mathrm{d}x = \int_{\alpha}^{\beta} (f \circ \varphi)(t)\varphi'(t)\ \mathrm{d}t.$$

Proposition 7.10. *$f : I \to \mathbb{K}$ $\mathcal{C}^0$ sur I intervalle. $(a, b) \in I^2$ avec $(-a) \in I$.*

$$\int_a^b f(x)\,\mathrm{d}x = \int_0^1 f((1-\lambda)a + \lambda b)(b-a)\,\mathrm{d}\lambda. \tag{i}$$

$$f \text{ } T\text{-périodique} \Longrightarrow \int_{a+T}^{b+T} f = \int_a^b f. \tag{ii}$$

$$f \text{ paire sur } [-a, a] \Longrightarrow \int_{-a}^{a} f = 2\int_0^a f. \tag{iii}$$

$$f \text{ impaire sur } [-a, a] \Longrightarrow \int_{-a}^{a} f = 0. \tag{iv}$$

Chapitre 8

Suites Réelles ou Complexes

I Quelques mots sur $\mathbb{R}$

Définition 8.1 ($\mathbb{Q}$)**.** *On définit une relation d'équivalence $\mathcal{R}$ sur $\mathbb{Z} \times \mathbb{N}^*$ par*

$$(p_1, q_1)\mathcal{R}(p_2, q_2) \iff p_1 q_2 = p_2 q_1.$$

On note alors

$$\mathbb{Q} = \{\mathrm{Cl}(m),\ m \in \mathbb{Z} \times \mathbb{N}^*\}.$$

Remarque 8.2. *On dit que $\mathbb{Z} \subset \mathbb{Q}$ au sens où il existe une injection de $\mathbb{Z}$ dans $\mathbb{Q}$ (par exemple $p \longmapsto \mathrm{Cl}(p, 1)$).*

Définition 8.3 (Propriété de la borne supérieure)**.** *Soit K un ensemble muni d'une relation d'ordre. On dit que K vérifie la* propriété de la borne supérieure *lorsque tout sous-ensemble non vide et majoré de K admet une borne supérieure.*

Proposition 8.4. *$(\mathbb{Q}, +, \times)$ est un corps commutatif, et $\leqslant$ est une relation d'ordre total sur $\mathbb{Q}$, mais $\mathbb{Q}$ ne vérifie pas la propriété de la borne supérieure.*

Théorème 8.5. *Il existe un ensemble $\mathbb{R} \supset \mathbb{Q}$ tel que $(\mathbb{R}, +, \times)$ est un corps commutatif, $\leqslant$ est une relation d'ordre total sur $\mathbb{R}$, et $\mathbb{R}$ vérifie la* propriété de la borne supérieure*.*

Corollaire 8.6. *Soit A un sous-ensemble minoré de $\mathbb{R}$ non vide. Alors A admet une borne inférieure (dans $\mathbb{R}$).*

Corollaire 8.7. *$\mathbb{R}$ est archimédien au sens où*

$$\forall x \in \mathbb{R}_+^*,\ \forall y \in \mathbb{R}^+,\ \exists n \in \mathbb{N},\ 0 \leqslant y < nx.$$

Démonstration. Supposer par l'absurde $\mathbb{R}$ non archimédien. Poser x et y tels que $\forall n \in \mathbb{N},\ y \geqslant nx$, $\Delta = \{nx,\ n \in \mathbb{N}\}$ et $s = \sup \Delta$ (car Δ majoré). Montrer que $s - x$ majore Δ, ce qui est une contradiction. □

Définition 8.8 ($\overline{\mathbb{R}}$)**.** *On définit $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$, muni de $+$, $\times$ et $\leqslant$ définies ci-dessous (on appelle $\widetilde{+}$ et $\widetilde{\times}$ respectivement $+$ et $\times$ dans $\mathbb{R}$) :*

$+$	$-\infty$	$x_2 \in \mathbb{R}$	$+\infty$
$-\infty$	$-\infty$	$-\infty$	
$x_1 \in \mathbb{R}$	$-\infty$	$x_1 \widetilde{+} x_2$	$+\infty$
$+\infty$		$+\infty$	$+\infty$

$\times$	$-\infty$	$x_2 \in \mathbb{R}_-^*$	0	$x_2 \in \mathbb{R}_+^*$	$+\infty$
$-\infty$	$+\infty$	$+\infty$		$-\infty$	$-\infty$
$x_1 \in \mathbb{R}_-^*$	$+\infty$	$x_1 \widetilde{\times} x_2$	0	$x_1 \widetilde{\times} x_2$	$-\infty$
0		0	0	0	
$x_1 \in \mathbb{R}_+^*$	$-\infty$	$x_1 \widetilde{\times} x_2$	0	$x_1 \widetilde{\times} x_2$	$+\infty$
$+\infty$	$-\infty$	$-\infty$		$+\infty$	$+\infty$

$\forall x \in \mathbb{R},\ -\infty \leqslant x \leqslant +\infty$	$-\infty \leqslant +\infty$

Proposition 8.9. *Toute partie non vide de $\overline{\mathbb{R}}$ admet une borne supérieure dans $\overline{\mathbb{R}}$.*

Définition 8.10 (Intervalle)**.** *Soit $I \subset \mathbb{R}$. On dit que I est un* intervalle *de $\mathbb{R}$ si I peut s'écrire sous la forme $[a,b]$, $[a,b[$, $]a,b]$ ou $]a,b[$, avec $(a,b) \in \overline{\mathbb{R}}^2$.*

Définition 8.11 (Convexe)**.** *Soit $C \subset \mathbb{R}^n$ (ou $\mathbb{C}$), $C \neq \varnothing$. C est dit* convexe *de $\mathbb{R}^n$ (ou $\mathbb{C}$) lorsque*

$$\forall (a,b) \in C^2,\ [a,b] \subset C.$$

Proposition 8.12. *Les intervalles de $\mathbb{R}$ sont les convexes de $\mathbb{R}$.*

II Notions de limites de suites et premières propriétés

II.1 Généralités sur les suites

Définition 8.13. *Une* suite *de réels ou de complexes est une application de $A \subset \mathbb{N}$, $A \neq \varnothing$ dans $\mathbb{K}$. La suite $u : A \to \mathbb{K}$ est notée $(u_n)_{n\in A}$.*

Définition 8.14. *Soit $(u_n)_{n\in\mathbb{N}}$ une suite de réels. On pose $A = \{u_n,\ n \in \mathbb{N}\}$.*

(i) *$(u_n)_{n\in\mathbb{N}}$ est* minorée *(resp.* majorée, bornée*) si A est minoré (resp. majoré, borné).*

(ii) *$(u_n)_{n\in\mathbb{N}}$ est* croissante *(resp.* décroissante*) si $\forall n \in \mathbb{N},\ u_{n+1} \geqslant u_n$ (resp. $u_{n+1} \leqslant u_n$).*

(iii) *$(u_n)_{n\in\mathbb{N}}$ est* périodique *si $\exists T \in \mathbb{N}^*,\ \forall n \in \mathbb{N},\ u_{n+T} = u_n$.*

(iv) *$(u_n)_{n\in\mathbb{N}}$ est* stationnaire *si $\exists n_0 \in \mathbb{N},\ \forall n \geqslant n_0,\ u_n = u_{n_0}$.*

Remarque 8.15. *Si $(u_n)_{n\in\mathbb{N}}$ est une suite de complexes, les définitions de périodicité et de stationnarité restent valables. Et on dit que $(u_n)_{n\in\mathbb{N}}$ est bornée lorsque $(|u_n|)_{n\in\mathbb{N}}$ est bornée.*

II.2 Définitions de limites

Définition 8.16 (Convergence)**.** *Soit $(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$, $\ell \in \mathbb{K}$. On dit que $(u_n)_{n\in\mathbb{N}}$* converge *vers ℓ lorsque*

$$\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N},\ \forall n \geqslant n_0,\ |u_n - \ell| \leqslant \varepsilon.$$

ℓ est dite limite de la suite $(u_n)_{n\in\mathbb{N}}$, et on note $u_n \xrightarrow[n\to+\infty]{} \ell$.

Proposition 8.17. *$(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$, $\ell \in \mathbb{K}$. $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ* ssi *pour tout $\varepsilon > 0$, $\{x \in \mathbb{K}, |x - \ell| \leqslant \varepsilon\}$ contient tous les termes de $(u_n)_{n\in\mathbb{N}}$ sauf un nombre fini.*

Proposition 8.18. *$(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$, $\ell \in \mathbb{K}$.*

$$u_n \xrightarrow[n\to+\infty]{} \ell \Longrightarrow \begin{cases} (u_n - \ell) \xrightarrow[n\to+\infty]{} 0 \\ (u_{n+1} - u_n) \xrightarrow[n\to+\infty]{} 0 \\ (u_n)_{n\in\mathbb{N}} \text{ bornée} \end{cases}.$$

Proposition 8.19. *$(u_n)_{n\in\mathbb{N}}$ une suite complexe.*

$$(u_n)_{n\in\mathbb{N}} \text{ converge} \iff \begin{cases} (\Re(u_n))_{n\in\mathbb{N}} \text{ converge} \\ (\Im(u_n))_{n\in\mathbb{N}} \text{ converge} \end{cases}.$$

Définition 8.20 (Divergence)**.** *Soit $(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$. On dit que* $(u_n)_{n\in\mathbb{N}}$ diverge *lorsque $(u_n)_{n\in\mathbb{N}}$ ne converge pas.*

Définition 8.21 (Limites infinies)**.** *Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. On définit :*

$$u_n \xrightarrow[n\to+\infty]{} +\infty \iff \forall A \in \mathbb{R}^+,\ \exists n_0 \in \mathbb{N},\ \forall n \geqslant n_0,\ u_n \geqslant A. \tag{i}$$

$$u_n \xrightarrow[n\to+\infty]{} -\infty \iff \forall A \in \mathbb{R}^-,\ \exists n_0 \in \mathbb{N},\ \forall n \geqslant n_0,\ u_n \leqslant A. \tag{ii}$$

Remarque 8.22. *Si $(u_n)_{n\in\mathbb{N}}$ est une suite complexe, on dit que $u_n \xrightarrow[n\to+\infty]{} +\infty$ lorsque $|u_n| \xrightarrow[n\to+\infty]{} +\infty$.*

Lemme 8.23. *$(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$ de limite $\pm\infty$. Alors $(u_n)_{n\in\mathbb{N}}$ n'est pas bornée.*

Proposition 8.24. *$(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$. Si $(u_n)_{n\in\mathbb{N}}$ admet une limite dans $\mathbb{K}\cup\{-\infty,+\infty\}$, alors cette limite est unique.*

Proposition 8.25. *Une suite d'éléments de $\mathbb{Z}$ convergente est stationnaire.*

II.3 Densité dans $\mathbb{R}$

Définition 8.26 (Densité)**.** *Soit $A \subset \mathbb{R}$. On dit que A est* dense *dans $\mathbb{R}$ lorsque, pour tout intervalle ouvert I de $\mathbb{R}$, $I \cap A \neq \varnothing$.*

Proposition 8.27. *$A \subset \mathbb{R}$. A est dense dans $\mathbb{R}$* ssi *tout réel est limite d'une suite d'éléments de A.*

Démonstration. ($\Rightarrow$) Pour $x \in \mathbb{R}, n \in \mathbb{N}^*$, poser $a_n \in \left]x-\frac{1}{n}, x+\frac{1}{n}\right[\cap A$ (a_n existe par la densité de A). On a alors $a_n \xrightarrow[n\to+\infty]{} x$. ($\Leftarrow$) Pour $(a,b) \in \mathbb{R}^2$, $a<b$, $\frac{a+b}{2}$ est limite d'une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A. Revenir à la définition de limite, poser $\varepsilon = \frac{b-a}{2}$ et en déduire $a_{n_0} \in]a,b[\cap A$. □

Proposition 8.28. *$\forall y \in \mathbb{R},\ \exists n \in \mathbb{Z},\ n \leqslant y < n+1$. On note $n = \lfloor y \rfloor$.*

Démonstration. Utiliser le fait que $\mathbb{R}$ est archimédien. □

Proposition 8.29. *$\mathbb{D} = \left\{\frac{k}{10^n},\ (k,n) \in \mathbb{Z}\times\mathbb{N}\right\}$ est dense dans $\mathbb{R}$. Ainsi, comme $\mathbb{Q} \supset \mathbb{D}$, $\mathbb{Q}$ est dense dans $\mathbb{R}$.*

Proposition 8.30. *$\mathbb{R}\backslash\mathbb{Q}$ est dense dans $\mathbb{R}$.*

Vocabulaire 8.31. *Pour $x \in \mathbb{R}$, $n \in \mathbb{N}$, $\frac{\lfloor 10^n x\rfloor}{10^n}$ est dite valeur approchée de x par défaut à 10^{-n} près et $\frac{\lfloor 10^n x\rfloor+1}{10^n}$ valeur approchée par excès.*

III Suites monotones

Théorème 8.32. *Soit $(u_n)_{n\in\mathbb{N}}$ une suite de réels.*

$$(u_n)_{n\in\mathbb{N}} \nearrow \Longrightarrow u_n \xrightarrow[n\to+\infty]{} \sup_{n\in\mathbb{N}} u_n \text{ (éventuellement } +\infty). \tag{i}$$

$$(u_n)_{n\in\mathbb{N}} \searrow \Longrightarrow u_n \xrightarrow[n\to+\infty]{} \inf_{n\in\mathbb{N}} u_n \text{ (éventuellement } -\infty). \tag{ii}$$

Définition 8.33 (Suites adjacentes)**.** *Soit $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites de réels. On dit que $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont* adjacentes *lorsque $(u_n)_{n\in\mathbb{N}} \nearrow$, $(v_n)_{n\in\mathbb{N}} \searrow$ et $v_n - u_n \xrightarrow[n\to+\infty]{} 0$.*

Proposition 8.34. *$(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites adjacentes. Alors $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ convergent vers une même limite notée ℓ et $\forall n \in \mathbb{N}$, $\ell \in [u_n, v_n]$.*

IV Opérations et limites

IV.1 Opérations

Lemme 8.35. *$(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ deux suites telles que $a_n \xrightarrow[n\to+\infty]{} 0$ et $(b_n)_{n\in\mathbb{N}}$ bornée. Alors $a_n b_n \xrightarrow[n\to+\infty]{} 0$.*

Proposition 8.36. *$(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites de réels.*

$$u_n \xrightarrow[n\to+\infty]{} \ell_1 \in \overline{\mathbb{R}} \Longrightarrow |u_n| \xrightarrow[n\to+\infty]{} |\ell_1|. \tag{i}$$

$$\left.\begin{array}{l} u_n \xrightarrow[n\to+\infty]{} \ell_1 \in \overline{\mathbb{R}} \\ v_n \xrightarrow[n\to+\infty]{} \ell_2 \in \overline{\mathbb{R}} \end{array}\right\} \Longrightarrow u_n + v_n \xrightarrow[n\to+\infty]{} \ell_1 + \ell_2 \quad (\text{si } \ell_1 + \ell_2 \text{ existe}). \tag{ii}$$

$$\left.\begin{array}{l} u_n \xrightarrow[n\to+\infty]{} \ell_1 \in \overline{\mathbb{R}} \\ v_n \xrightarrow[n\to+\infty]{} \ell_2 \in \overline{\mathbb{R}} \end{array}\right\} \Longrightarrow u_n v_n \xrightarrow[n\to+\infty]{} \ell_1\ell_2 \quad (\text{si } \ell_1\ell_2 \text{ existe}). \tag{iii}$$

$$u_n \xrightarrow[n\to+\infty]{} \ell \in \overline{\mathbb{R}} \Longrightarrow \frac{1}{u_n} \xrightarrow[n\to+\infty]{} \begin{cases} \frac{1}{\ell} \text{ si } \ell \in \mathbb{R}^* \\ +\infty \text{ si } \ell = 0 \text{ et } u_n \geqslant 0 \text{ à PCR} \\ -\infty \text{ si } \ell = 0 \text{ et } u_n \leqslant 0 \text{ à PCR} \\ 0 \text{ si } \ell = \pm\infty \end{cases}. \tag{iv}$$

Remarque 8.37. *Dans $\mathbb{C}$, la formule* (i) *reste valable. La formule* (ii) *est valable à condition que ℓ_1 et ℓ_2 ne soient pas tous deux infinis.*

Proposition 8.38. *P, Q deux fonctions polynomiales non nulles de degrés $p \geqslant 0$, $q \geqslant 0$ et de coefficients dominants a_p et b_q. Alors les suites $\left(\frac{P(n)}{Q(n)}\right)_{n\in\mathbb{N}}$ et $\left(\frac{a_p n^p}{b_q n^q}\right)_{n\in\mathbb{N}}$ ont la même limite dans $\overline{\mathbb{R}}$.*

IV.2 Propriétés liées à l'ordre

Proposition 8.39. *$(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ et $(w_n)_{n\in\mathbb{N}}$ trois suites de réels.*

$$\left.\begin{array}{l} u_n \xrightarrow[n\to+\infty]{} \ell_1 \in \overline{\mathbb{R}} \\ v_n \xrightarrow[n\to+\infty]{} \ell_2 \in \overline{\mathbb{R}} \\ u_n \leqslant v_n \text{ à PCR} \end{array}\right\} \Longrightarrow \ell_1 \leqslant \ell_2. \tag{i}$$

$$\left.\begin{array}{r} u_n \xrightarrow[n\to+\infty]{} +\infty \\ u_n \leqslant v_n \text{ à } PCR \end{array}\right\} \Longrightarrow v_n \xrightarrow[n\to+\infty]{} +\infty. \tag{ii}$$

$$\left.\begin{array}{r} v_n \xrightarrow[n\to+\infty]{} -\infty \\ u_n \leqslant v_n \text{ à } PCR \end{array}\right\} \Longrightarrow u_n \xrightarrow[n\to+\infty]{} -\infty. \tag{iii}$$

$$\left.\begin{array}{r} u_n \xrightarrow[n\to+\infty]{} \ell \in \overline{\mathbb{R}} \\ w_n \xrightarrow[n\to+\infty]{} \ell \\ u_n \leqslant v_n \leqslant w_n \text{ à } PCR \end{array}\right\} \Longrightarrow v_n \xrightarrow[n\to+\infty]{} \ell. \tag{iv}$$

$$u_n \xrightarrow[n\to+\infty]{} \ell \in \overline{\mathbb{R}}^* \Longrightarrow u_n \text{ est du signe de } \ell \text{ à } PCR. \tag{v}$$

Proposition 8.40 (Critère de d'Alembert)**.** *$(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{R}_+^*$ t.q. $\frac{u_{n+1}}{u_n} \xrightarrow[n\to+\infty]{} \ell \in \mathbb{R}$. Alors :*

(i) *Si $\ell < 1$, alors $u_n \xrightarrow[n\to+\infty]{} 0$.*

(ii) *Si $\ell = 1$, alors $(u_n)_{n\in\mathbb{N}}$ peut converger ou diverger.*

(iii) *Si $\ell > 1$, alors $u_n \xrightarrow[n\to+\infty]{} +\infty$.*

Notation 8.41 (Diamètre)**.** *Soit I un segment. On note $\delta(I)$ son* diamètre *: $\delta(I) = \sup I - \inf I$.*

Théorème 8.42 (Théorème des segments emboîtés)**.** *$(K_n)_{n\in\mathbb{N}}$ une suite de segments emboîtés : $\forall n \in \mathbb{N}$, $K_{n+1} \subset K_n$ et $\delta(K_n) \xrightarrow[n\to+\infty]{} 0$. Alors*

$$\exists \ell \in \mathbb{R}, \bigcap_{n\in\mathbb{N}} K_n = \{\ell\}.$$

Démonstration. Poser $K_n = [a_n, b_n]$ pour tout n et montrer que $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont des suites adjacentes. □

V Écriture décimale et conséquences

V.1 Retour sur les suites géométriques

Proposition 8.43. *$q \in \mathbb{C}$. $u_n = q^n$ et $S_n = \sum_{k=0}^n q^k$ pour tout $n \in \mathbb{N}$.*

$$\left\{\begin{array}{l} |q| < 1 \Longrightarrow u_n \xrightarrow[n\to+\infty]{} 0 \\ q = 1 \Longrightarrow (u_n)_{n\in\mathbb{N}} \text{ constante} \\ |q| = 1 \text{ et } q \neq 1 \Longrightarrow (u_n)_{n\in\mathbb{N}} \text{ diverge} \\ |q| > 1 \Longrightarrow u_n \xrightarrow[n\to+\infty]{} +\infty \end{array}\right. . \tag{i}$$

$$(S_n)_{n\in\mathbb{N}} \text{ converge} \Longleftrightarrow |q| < 1. \tag{ii}$$

V.2 Écriture décimale d'un réel

Définition 8.44 (Décimales d'un réel)**.** *$x \in \mathbb{R}$. On définit la suite $(a_k)_{k\in\mathbb{N}}$ des* décimales *de x par*

$$\left\{\begin{array}{l} a_0 = \lfloor x \rfloor \\ \forall k \in \mathbb{N}^*, \ a_k = \lfloor 10^k x \rfloor - 10 \lfloor 10^{k-1} x \rfloor \end{array}\right. .$$

Lemme 8.45. *$(\alpha_k)_{k\in\mathbb{N}}$ une suite d'entiers de $[\![0,9]\!]$. $n\in\mathbb{N}$.*

$$\sum_{k=n+1}^{N}\frac{\alpha_k}{10^k}\xrightarrow[N\to+\infty]{} R_n\in\left[0,\frac{1}{10^n}\right], \tag{i}$$

$$R_n=\frac{1}{10^n}\iff\forall k\geqslant n+1,\ \alpha_k=9. \tag{ii}$$

Proposition 8.46 (Existence d'un réel associé à une écriture décimale)**.** *Soit $(a_k)_{k\in\mathbb{N}}$ une suite d'entiers telle que $\forall k\in\mathbb{N}^*$, $a_k\in[\![0,9]\!]$ et $\exists k\in\mathbb{N}^*$, $a_k\neq 9$. Alors*

$$\sum_{k=0}^{N}\frac{a_k}{10^k}\xrightarrow[N\to+\infty]{} x\in[a_0,a_0+1[.$$

Le réel x est noté $a_0,a_1a_2\cdots a_k\cdots$.

Théorème 8.47 (Existence et unicité de l'écriture décimale d'un réel)**.** *$x\in\mathbb{R}$. $(a_k)_{k\in\mathbb{N}}$ la suite des décimales de x (c.f. définition 8.44).*

$$\forall k\in\mathbb{N}^*,\ a_k\in[\![0,9]\!]. \tag{i}$$

$$\forall n_0\in\mathbb{N},\ \exists n\geqslant n_0,\ a_n\neq 9. \tag{ii}$$

$$\sum_{k=0}^{N}\frac{a_k}{10^k}=\frac{\lfloor 10^N x\rfloor}{10^N}\xrightarrow[N\to+\infty]{} x. \tag{iii}$$

La suite $(a_k)_{k\in\mathbb{N}}$ est la seule vérifiant (i)*,* (ii) *et* (iii)*.* (iv)

Démonstration. (i) Revenir à la définition 8.44 et écrire les inégalités caractérisant les parties entières. (ii) Par l'absurde. (iii) Poser $u_k=\frac{\lfloor 10^k x\rfloor}{10^k}$, montrer que $\frac{a_k}{10^k}=u_k-u_{k-1}$, puis utiliser une somme télescopique pour calculer $\sum_{k=1}^{N}\frac{a_k}{10^k}=u_N-u_0$. (iv) Prendre $(a_k)_{k\in\mathbb{N}}$ une suite vérifiant les trois propriétés. Poser $\rho_n=x-\sum_{k=0}^{n}\frac{a_k}{10^k}$ pour tout n. Montrer que $\sum_{k=n+1}^{N}\frac{a_k}{10^k}\xrightarrow[N\to+\infty]{}\rho_n$. Déduire du lemme 8.45 que $\rho_n\in\left[0,\frac{1}{10^n}\right[$. Montrer alors que $a_0=\lfloor x\rfloor$ puis montrer par récurrence forte sur k que $\forall k\in\mathbb{N}^*$, $a_k=\lfloor 10^k x\rfloor-10\lfloor 10^{k-1}x\rfloor$. □

V.3 Non dénombrabilité de $\mathbb{R}$

Définition 8.48 (Dénombrabilité)**.** *Un ensemble est dit* dénombrable *lorsqu'il est en bijection avec $\mathbb{N}$.*

Proposition 8.49. *$[0,1]$ est non dénombrable.*

Démonstration (Première méthode)**.** Par l'absurde : supposer qu'il existe une bijection $\varphi:\mathbb{N}\to[0,1]$, et noter $u_n=\varphi(n)$. On a alors $[0,1]=\{u_n,\ n\in\mathbb{N}\}$. Définir une suite de segments emboîtés $(I_n)_{n\in\mathbb{N}}$ comme suit. Parmi $\left[0,\frac{1}{3}\right]$, $\left[\frac{1}{3},\frac{2}{3}\right]$ et $\left[\frac{2}{3},1\right]$, au moins un ne contient pas u_0, on le note I_0. On suppose avoir construit les $(n+1)$ premiers termes de $(I_n)_{n\in\mathbb{N}}$ avec $\delta(I_n)=3^{-n-1}$, $u_n\notin I_n$ et $I_n\subset I_{n-1}$. On "coupe" alors I_n en trois segments, dont l'un ne contient pas u_{n+1} et on note ce segment I_{n+1}. On a alors bien $\delta(I_{n+1})=3^{-n-2}$, $u_{n+1}\notin I_{n+1}$ et $I_{n+1}\subset I_n$. Par le théorème des segments emboîtés : $\exists\ell\in\mathbb{R}$, $\bigcap_{n\in\mathbb{N}}I_n=\{\ell\}$. Donc $\ell\in[0,1]$ mais $\ell\notin\{u_n,\ n\in\mathbb{N}\}$. Contradiction. □

Démonstration (Deuxième méthode)**.** Par l'absurde : supposer qu'il existe une bijection $\varphi : \mathbb{N}^* \to [0,1[$, et noter $u_n = \varphi(n)$. On a alors $[0,1[= \{u_n,\, n \in \mathbb{N}^*\}$. Pour $n \in \mathbb{N}^*$, noter a_n la n-ième décimale de u_n. Définir alors la suite $(b_n)_{n\in\mathbb{N}}$ par $b_0 = 0$ et

$$\forall n \in \mathbb{N}^*,\ \begin{cases} b_n = 1 & \text{si } a_n \neq 1 \\ b_n = 2 & \text{sinon} \end{cases}.$$

Appeler alors x le réel dont la suite de décimales est $(b_n)_{n\in\mathbb{N}}$ et montrer que $x \in [0,1[$ mais $x \notin \{u_n,\, n \in \mathbb{N}^*\}$. Contradiction. □

Proposition 8.50. *Tout intervalle de $\mathbb{R}$ est non dénombrable.*

Démonstration. Montrer que les bijections suivantes existent : $[0,1[\to [0,1]$, $]-1,1[\to [-1,1]$, $(a,b) \to (0,1)$, $\mathbb{R} \to \left]-\frac{\pi}{2},\frac{\pi}{2}\right[$, $\mathbb{R}_+ \to \left[0,\frac{\pi}{2}\right[$, $\mathbb{R}_- \to \left]-\frac{\pi}{2},0\right]$, $(a,+\infty[\to \mathbb{R}_+$ et $]-\infty,a) \to \mathbb{R}_-$. □

Conjecture 8.51 (Hypothèse du continu)**.** *Tout sous-ensemble de $\mathbb{R}$ est soit en bijection avec $\mathbb{R}$, soit dénombrable, soit fini.*

VI Sous-suites

Définition 8.52 (Sous-suites)**.** *$(u_n)_{n\in\mathbb{N}}$ une suite de réels ou de complexes. On appelle* sous-suite *(ou* suite extraite*) de $(u_n)_{n\in\mathbb{N}}$ toute suite du type $\left(u_{\varphi(n)}\right)_{n\in\mathbb{N}}$, où $\varphi : \mathbb{N} \to \mathbb{N}$ ↗↗ est dite* extractrice*.*

Proposition 8.53. *$(u_n)_{n\in\mathbb{N}}$ une suite de réels ou de complexes.*

$$(u_n)_{n\in\mathbb{N}} \text{ converge} \iff (u_{2n})_{n\in\mathbb{N}} \text{ et } (u_{2n+1})_{n\in\mathbb{N}} \text{ convergent vers la même limite.}$$

Lemme 8.54. $\varphi : \mathbb{N} \to \mathbb{N}$ ↗↗. $\forall n \in \mathbb{N}$, $\varphi(n) \geqslant n$.

Proposition 8.55. *$(u_n)_{n\in\mathbb{N}}$ une suite de réels ou de complexes. $(u_n)_{n\in\mathbb{N}}$ admet une limite* ssi *toute sous-suite de $(u_n)_{n\in\mathbb{N}}$ admet une limite (qui est alors égale à $\lim_{n\to+\infty} u_n$).*

Théorème 8.56 (Théorème de Bolzano-Weierstrass)**.** *Si $(u_n)_{n\in\mathbb{N}}$ est une suite réelle ou complexe bornée, alors il existe une sous-suite de $(u_n)_{n\in\mathbb{N}}$ qui converge.*

Démonstration. Dans un premier temps, supposer $(u_n)_{n\in\mathbb{N}}$ réelle. Construire une suite de segments emboîtés $(I_n)_{n\in\mathbb{N}}$ comme suit. On pose $I_0 = [m,M]$, où m et M sont respectivement un minorant et un majorant de $(u_n)_{n\in\mathbb{N}}$. On suppose avoir construit les $(n+1)$ premiers termes de la suite $(I_n)_{n\in\mathbb{N}}$ tels que $I_n \subset I_{n-1}$, $\delta(I_n) = \frac{1}{2}\delta(I_{n-1})$ et l'ensemble $\{k \in \mathbb{N},\, u_k \in I_n\}$ est infini. Parmi les segments $\left[\inf I_n, \frac{\inf I_n + \sup I_n}{2}\right]$ et $\left[\frac{\inf I_n + \sup I_n}{2}, \sup I_n\right]$ au moins un contient une infinité de termes de la suite ; on le note I_{n+1}. On a donc construit $(I_n)_{n\in\mathbb{N}}$ tel que $\exists \ell \in \mathbb{R}, \bigcap_{n\in\mathbb{N}} I_n = \{\ell\}$. Chercher alors $\varphi : \mathbb{N} \to \mathbb{N}$ ↗↗ tel que $u_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell$. Pour cela, choisir $\varphi(0) = 0$, puis supposer avoir construit $\varphi(0) < \cdots < \varphi(n)$ tel que $\forall k \in [\![0,n]\!]$, $u_{\varphi(k)} \in I_k$. Poser enfin $\varphi(n+1) = \min\{k > \varphi(n),\, u_k \in I_{n+1}\}$, puis vérifier que $u_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell$. Dans le cas complexe, se ramener au cas réel en posant $a_n = \Re(u_n)$, $b_n = \Im(u_n)$ et trouver φ et ψ tels que $\left(a_{(\varphi\circ\psi)(n)}\right)_{n\in\mathbb{N}}$ et $\left(b_{(\varphi\circ\psi)(n)}\right)_{n\in\mathbb{N}}$ convergent. □

Vocabulaire 8.57. *$(u_n)_{n\in\mathbb{N}}$ une suite de réels. Les limites réelles des suites extraites de $(u_n)_{n\in\mathbb{N}}$ sont dites* valeurs adhérentes *de $(u_n)_{n\in\mathbb{N}}$.*

VII Exemples de suites récurrentes

VII.1 Suites arithmético-géométriques

Définition 8.58 (Suites arithmético-géométriques)**.** $(a,b) \in \mathbb{C}^2$. *On appelle* suite arithmético-géométrique *toute suite* $(u_n)_{n\in\mathbb{N}}$ *telle que*

$$\forall n \in \mathbb{N},\ u_{n+1} = au_n + b.$$

Proposition 8.59. $(a,b) \in \mathbb{C}^2$, $a \neq 1$, $b \neq 0$. $(u_n)_{n\in\mathbb{N}}$ *vérifiant* $\forall n \in \mathbb{N},\ u_{n+1} = au_n + b$.

$$(u_n)_{n\in\mathbb{N}} \text{ converge} \iff |a| < 1 \text{ ou } u_0 = au_0 + b.$$

Dans le cas où $(u_n)_{n\in\mathbb{N}}$ *converge, on a* $u_n \xrightarrow[n\to+\infty]{} \frac{b}{1-a}$.

VII.2 Suites récurrentes linéaires à deux termes

Proposition 8.60. $(a,b) \in \mathbb{K} \times \mathbb{K}^*$. *On cherche les* $(u_n)_{n\in\mathbb{N}}$ *suites d'éléments de* $\mathbb{K}$ *telles que*

$$\forall n \in \mathbb{N},\ u_{n+2} = au_{n+1} + bu_n. \tag{$*$}$$

On appelle équation caractéristique de $(*)$ *l'équation*

$$r^2 = ar + b. \tag{$**$}$$

On appelle Δ *le discriminant de* $(**)$ *et* r_1 *et* r_2 *ses deux racines, et on note* ϑ *un argument de* r_1. *On a alors*

$$(u_n)_{n\in\mathbb{N}} \text{ vérifie } (*) \iff \exists(\lambda,\mu) \in \mathbb{K}^2,\ \forall n \in \mathbb{N},\ u_n = \lambda\alpha_n + \mu\beta_n,$$

où $(\alpha_n)_{n\in\mathbb{N}}$ *et* $(\beta_n)_{n\in\mathbb{N}}$ *sont définies ci-dessous :*

<table>
<tr><th></th><th>$\Delta \in \mathbb{R}_+$</th><th>$\Delta = 0$</th><th>$\Delta \in \mathbb{C}\backslash\mathbb{R}_+$</th></tr>
<tr><td>$\mathbb{K} = \mathbb{C}$</td><td rowspan="2">$\alpha_n = (r_1)^n$
$\beta_n = (r_2)^n$</td><td rowspan="2">$\alpha_n = (r_1)^n$
$\beta_n = n\,(r_1)^n$</td><td>$\alpha_n = (r_1)^n$
$\beta_n = (r_2)^n$</td></tr>
<tr><td>$\mathbb{K} = \mathbb{R}$</td><td>$\alpha_n = \lvert r_1\rvert^n \cos(n\vartheta)$
$\beta_n = \lvert r_1\rvert^n \sin(n\vartheta)$</td></tr>
</table>

Démonstration. Poser $v_n = \frac{u_n}{(r_1)^n}$, ce qui est possible car $b \neq 0$ donc $r_1 \neq 0$. Poser ensuite $w_n = v_{n+1} - v_n$. Montrer alors que $\forall n \in \mathbb{N},\ w_{n+1} = \left(\frac{r_2}{r_1}\right) w_n$. En distinguant les cas $\Delta = 0$ ou $\Delta \neq 0$ et $\mathbb{K} = \mathbb{C}$ ou $\mathbb{K} = \mathbb{R}$, montrer le résultat voulu. □

VIII Relations de comparaison

VIII.1 Généralités

Définition 8.61 (o, $\mathcal{O}$ et $\sim$)**.** $(u_n)_{n\in\mathbb{N}}$ *et* $(v_n)_{n\in\mathbb{N}}$ *deux suites réelles.*

(i) *On dit que* $u_n = o(v_n)$ *lorsqu'il existe* $(\varepsilon_n)_{n\in\mathbb{N}}$ *de limite* 0 *telle que* $u_n = \varepsilon_n v_n$ *à PCR.*

(ii) *On dit que* $u_n = \mathcal{O}(v_n)$ *lorsqu'il existe* $(\phi_n)_{n\in\mathbb{N}}$ *bornée telle que* $u_n = \phi_n v_n$ *à PCR.*

(iii) *On dit que* $u_n \sim v_n$ *lorsqu'il existe* $(\psi_n)_{n\in\mathbb{N}}$ *de limite* 1 *telle que* $u_n = \psi_n v_n$ *à PCR.*

Proposition 8.62. $(u_n)_{n\in\mathbb{N}}$ *et* $(v_n)_{n\in\mathbb{N}}$ *deux suites réelles.*

$$u_n = o(1) \iff u_n \xrightarrow[n\to+\infty]{} 0. \tag{i}$$

$$u_n \sim v_n \iff u_n - v_n = o(v_n). \tag{ii}$$

$$u_n = o(v_n) \implies u_n = \mathcal{O}(v_n). \tag{iii}$$

VIII.2 Opérations

Proposition 8.63. $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$, $(w_n)_{n\in\mathbb{N}}$ *et* $(x_n)_{n\in\mathbb{N}}$ *quatre suites réelles.* $\alpha \in \mathbb{R}$.

$$\left.\begin{array}{r} u_n = \mathcal{O}(w_n) \\ v_n = \mathcal{O}(w_n) \\ w_n \sim x_n \end{array}\right\} \implies \left\{\begin{array}{l} u_n + v_n = \mathcal{O}(w_n) \\ u_n v_n = \mathcal{O}(w_n^2) \\ \alpha u_n = \mathcal{O}(w_n) \\ u_n = \mathcal{O}(x_n) \end{array}\right. .$$

Cette propriété reste valable en remplaçant $\mathcal{O}$ *par* o.

Proposition 8.64. $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$, $(x_n)_{n\in\mathbb{N}}$ *et* $(y_n)_{n\in\mathbb{N}}$ *quatre suites réelles.* $\alpha \in \mathbb{R}_+^*$.

$$\left.\begin{array}{r} u_n \sim v_n \\ x_n \sim y_n \end{array}\right\} \implies \left\{\begin{array}{l} u_n x_n \sim v_n y_n \\ \frac{u_n}{x_n} \sim \frac{v_n}{y_n} \\ (u_n)^\alpha \sim (v_n)^\alpha \end{array}\right. ,$$

à condition que les expressions aient un sens (en particulier pour le quotient et la puissance).

VIII.3 Applications

Proposition 8.65. $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ *et* $(w_n)_{n\in\mathbb{N}}$ *trois suites réelles.* $\ell \in \mathbb{R}$.

$$u_n \xrightarrow[n\to+\infty]{} \ell \neq 0 \implies u_n \sim \ell. \tag{i}$$

$$\left.\begin{array}{r} u_n \sim v_n \\ v_n \xrightarrow[n\to+\infty]{} \ell \end{array}\right\} \implies u_n \xrightarrow[n\to+\infty]{} \ell. \tag{ii}$$

$$\left.\begin{array}{r} u_n \leqslant v_n \leqslant w_n \text{ à PCR} \\ u_n \sim w_n \end{array}\right\} \implies u_n \sim v_n. \tag{iii}$$

VIII.4 Quelques identités

Proposition 8.66. $(u_n)_{n\in\mathbb{N}}$ *une suite réelle avec* $u_n \xrightarrow[n\to+\infty]{} 0$. $\alpha \in \mathbb{R}$.

$$\sin u_n = u_n + \mathcal{O}(u_n^3), \tag{i}$$

$$\cos u_n = 1 - \frac{u_n^2}{2} + \mathcal{O}(u_n^4), \tag{ii}$$

$$\tan u_n = u_n + \mathcal{O}(u_n^3), \tag{iii}$$

$$e^{u_n} = 1 + u_n + \mathcal{O}(u_n^2), \tag{iv}$$

$$\ln(1 + u_n) = u_n + \mathcal{O}(u_n^2), \tag{v}$$

$$(1 + u_n)^\alpha = 1 + \alpha u_n + \mathcal{O}(u_n^2). \tag{vi}$$

Chapitre 9

Limites et Fonctions

I Notations

Définition 9.1 (Voisinage)**.** $x_0 \in \mathbb{R}$. *On appelle* voisinage de x_0 *toute partie de* $\mathbb{R}$ *contenant un intervalle ouvert centré en* x_0. *On appelle de plus* voisinage de $+\infty$ *(resp.* $-\infty$*) toute partie de* $\mathbb{R}$ *contenant un intervalle du type* $]M, +\infty[$ *(resp.* $]-\infty, M[$*), où* $M \in \mathbb{R}$.

Définition 9.2 (Adhérence)**.** $x_0 \in \overline{\mathbb{R}}$. $A \subset \mathbb{R}$. *On dit que* x_0 *est* adhérent *à* A *lorsque tout voisinage de* x_0 *rencontre* A.

Remarque 9.3. *On notera par la suite* $\mathcal{D}_f = I$ *ou* $I \backslash \{a\}$, *où* I *est un intervalle et* $a \in I \backslash \{\inf I, \sup I\}$. *On étudiera* $f : \mathcal{D}_f \to \mathbb{R}$ *en tout point* x_0 *adhérent à* $\mathcal{D}_f$.

Définition 9.4. *On dit que* $f : \mathcal{D}_f \to \mathbb{R}$ *vérifie une propriété* au voisinage de x_0 *lorsqu'il existe un voisinage* V *de* x_0 *tel que la propriété est vérifiée en tout point de* $V \cap \mathcal{D}_f$.

II Limite d'une fonction

II.1 Limites réelles

Définition 9.5 (Limite réelle)**.** $f : \mathcal{D}_f \to \mathbb{R}$. $\ell \in \mathbb{R}$. x_0 *adhérent à* $\mathcal{D}_f$.

(i) *Si* $x_0 \in \mathbb{R}$, *on dit que* $\lim_{x_0} f = \ell$ *lorsque*

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall x \in]x_0 - \eta, x_0 + \eta[\cap \mathcal{D}_f,\ |f(x) - \ell| \leqslant \varepsilon.$$

(ii) *Si* $x_0 = +\infty$, *on dit que* $\lim_{+\infty} f = \ell$ *lorsque*

$$\forall \varepsilon > 0,\ \exists M \in \mathbb{R}_+,\ \forall x \in]M, +\infty[,\ |f(x) - \ell| \leqslant \varepsilon.$$

(iii) *Si* $x_0 = -\infty$, *on dit que* $\lim_{-\infty} f = \ell$ *lorsque*

$$\forall \varepsilon > 0,\ \exists M \in \mathbb{R}_-,\ \forall x \in]-\infty, M[,\ |f(x) - \ell| \leqslant \varepsilon.$$

Proposition 9.6. $f : I \to \mathbb{R}$ *(définie sur tout l'intervalle* I*). Si* f *admet une limite* $\ell \in \mathbb{R}$ *en* $x_0 \in I$, *alors* $f(x_0) = \ell$.

Définition 9.7 (Continuité)**.** $f : I \to \mathbb{R}$ *(définie sur tout l'intervalle* I*). On dit que* f *est* $\mathcal{C}^0$ *en* $x_0 \in I$ *lorsque* f *admet une limite réelle* ℓ *en* x_0. *On dit de plus que* f *est* $\mathcal{C}^0$ *sur* $X \subset I$ *lorsque* f *est* $\mathcal{C}^0$ *en tout point de* X.

Définition 9.8 (Continuité à droite, à gauche)**.** $f : I \to \mathbb{R}$ *(définie sur tout l'intervalle I).*

(i) *On dit que f est $\mathcal{C}^0$* à droite *en $x_0 \in I \backslash \{\sup I\}$ lorsque $f_{|[x_0,+\infty[}$ est $\mathcal{C}^0$ en x_0.*

(ii) *On dit que f est $\mathcal{C}^0$* à gauche *en $x_0 \in I \backslash \{\inf I\}$ lorsque $f_{|]-\infty,x_0]}$ est $\mathcal{C}^0$ en x_0.*

II.2 Limites infinies

Définition 9.9 (Limite infinie)**.** $f : \mathcal{D}_f \to \mathbb{R}$. x_0 *adhérent à $\mathcal{D}_f$.*

(i) *Si $x_0 \in \mathbb{R}$, on dit que $\lim_{x_0} f = +\infty$ lorsque*

$$\forall M \in \mathbb{R}_+,\ \exists \eta > 0,\ \forall x \in]x_0 - \eta, x_0 + \eta[\cap \mathcal{D}_f,\ f(x) \geqslant M.$$

(ii) *Si $x_0 = +\infty$, on dit que $\lim_{+\infty} f = +\infty$ lorsque*

$$\forall M \in \mathbb{R}_+,\ \exists M' \in \mathbb{R}_+,\ \forall x \in]M', +\infty[,\ f(x) \geqslant M.$$

(iii) *Si $x_0 = -\infty$, on dit que $\lim_{-\infty} f = +\infty$ lorsque*

$$\forall M \in \mathbb{R}_+,\ \exists M' \in \mathbb{R}_-,\ \forall x \in]-\infty, M'[,\ f(x) \geqslant M.$$

Proposition 9.10. *$f : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$. Si f admet une limite réelle en x_0, alors f est bornée au voisinage de x_0.*

Proposition 9.11. *$f : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$. Si $\lim_{x_0} f = \pm\infty$ alors f est non bornée au voisinage de x_0.*

Proposition 9.12. *$f : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$. Si f admet une limite $\ell \in \overline{\mathbb{R}}$ en x_0, alors elle est unique.*

II.3 Limites à droite et à gauche

Définition 9.13 (Limite à droite, à gauche)**.** $f : \mathcal{D}_f \to \mathbb{R}$. $\ell \in \overline{\mathbb{R}}$. x_0 *adhérent à $\mathcal{D}_f$, $x_0 \neq \sup I$, $x_0 \neq \inf I$.*

(i) *On dit que $\lim_{x_0^+} f = \ell$ lorsque $\lim_{x_0} f_{]x_0,+\infty[} = \ell$.*

(ii) *On dit que $\lim_{x_0^-} f = \ell$ lorsque $\lim_{x_0} f_{]-\infty,x_0[} = \ell$.*

Proposition 9.14. *$f : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$. Si f admet une limite $\ell \in \overline{\mathbb{R}}$ en x_0, alors f admet une limite à droite et à gauche en x_0.*

Proposition 9.15. *$f : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$.*

(i) *Si $\mathcal{D}_f = I$, si f admet une limite à droite et à gauche en x_0 avec $f(x_0) = \lim_{x_0^-} f = \lim_{x_0^+} f$ alors f admet une limite en x_0.*

(ii) *Si $\mathcal{D}_f = I \backslash \{x_0\}$, si f admet une limite à droite et gauche en x_0 avec $\lim_{x_0^-} f = \lim_{x_0^+} f$ alors f admet une limite en x_0.*

II.4 Adhérence de la limite

Définition 9.16 (Définition équivalente de limite)**.** $f : \mathcal{D}_f \to \mathbb{R}$. $\ell \in \overline{\mathbb{R}}$. x_0 *adhérent à $\mathcal{D}_f$. On dit que $\lim_{x_0} f = \ell$ lorsque*

$$\forall V \text{ voisinage de } \ell,\ \exists W \text{ voisinage de } x_0,\ f(W \cap \mathcal{D}_f) \subset V.$$

Proposition 9.17. *$f : \mathcal{D}_f \to \mathbb{R}$. $\ell \in \overline{\mathbb{R}}$. x_0 adhérent à $\mathcal{D}_f$. Si $\lim_{x_0} f = \ell$, alors ℓ est adhérent à $f(\mathcal{D}_f)$.*

III Étude de $u_{n+1} = f(u_n)$

Proposition 9.18. *$f : \mathcal{D}_f \to \mathbb{R}$. $\ell \in \overline{\mathbb{R}}$. x_0 adhérent à $\mathcal{D}_f$.* $\lim_{x_0} f = \ell$ ssi *pour toute suite $(u_n)_{n\in\mathbb{N}}$ telle que $u_n \in \mathcal{D}_f$ à PCR et de limite x_0, $f(u_n) \xrightarrow[n\to+\infty]{} \ell$.*

Proposition 9.19. *$f : I \to \mathbb{R}$, avec $f(I) \subset I$. $u_0 \in I$. f $\mathcal{C}^0$ sur I. On définit $u_{n+1} = f(u_n)$ pour tout $n \in \mathbb{N}$. Alors $(u_n)_{n\in\mathbb{N}}$ est une suite d'éléments de I ; et si $u_n \xrightarrow[n\to+\infty]{} \ell \in I$, alors $f(\ell) = \ell$.*

Proposition 9.20. *$f : I \to \mathbb{R}$, avec $f(I) \subset I$. $u_0 \in I$. f $\mathcal{C}^0$ sur I. On définit $u_{n+1} = f(u_n)$ pour tout $n \in \mathbb{N}$.*

(i) *Si $f \nearrow$ sur I, alors $(u_n)_{n\in\mathbb{N}}$ est monotone.*

(ii) *Si $f \searrow$ sur I, alors $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$ sont monotones et de sens de variation contraires.*

IV Opérations et limites

Proposition 9.21. *$f, g : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$.* $\lim_{x_0} f = \ell_1 \in \overline{\mathbb{R}}$. $\lim_{x_0} g = \ell_2 \in \overline{\mathbb{R}}$.

$$\lim_{x_0} |f| = |\ell_1|, \tag{i}$$

$$\lim_{x_0} (f+g) = \ell_1 + \ell_2 \quad \textit{(si } \ell_1 + \ell_2 \textit{ existe)}, \tag{ii}$$

$$\lim_{x_0} (fg) = \ell_1\ell_2 \quad \textit{(si } \ell_1\ell_2 \textit{ existe)}, \tag{iii}$$

$$\lim_{x_0} \left(\frac{f}{g}\right) = \frac{\ell_1}{\ell_2} \quad \textit{(si } \frac{\ell_1}{\ell_2} \textit{ existe)}. \tag{iv}$$

Proposition 9.22. *$f, g : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$. Si* $\lim_{x_0} f = 0$ *et si g est bornée dans un voisinage de x_0 alors* $\lim_{x_0}(fg) = 0$.

Proposition 9.23. *$f : \mathcal{D}_f \to \mathbb{R}$. $g : J \to \mathbb{R}$, avec J intervalle, $J \supset f(\mathcal{D}_f)$. x_0 adhérent à $\mathcal{D}_f$.* $\lim_{x_0} f = \alpha \in \overline{\mathbb{R}}$. $\lim_{\alpha} g = \ell \in \overline{\mathbb{R}}$. *Alors* $\lim_{x_0}(g \circ f) = \ell$.

V Ordre et limite

Proposition 9.24. *$f, g : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$.* $\lim_{x_0} f = \ell_1 \in \overline{\mathbb{R}}$. $\lim_{x_0} g = \ell_2 \in \overline{\mathbb{R}}$. *Si $f \leqslant g$ dans un voisinage de x_0 intersecté avec $\mathcal{D}_f$, alors $\ell_1 \leqslant \ell_2$.*

Théorème 9.25 (Théorème de convergence par encadrement)**.** *$f, g, h : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$.*

$$\left.\begin{array}{r} f \leqslant g \leqslant h \textit{ dans un voisinage de } x_0 \\ \lim_{x_0} f = \lim_{x_0} h = \ell \in \mathbb{R} \end{array}\right\} \Longrightarrow \lim_{x_0} g = \ell. \tag{i}$$

$$\left.\begin{array}{r} f \leqslant g \textit{ dans un voisinage de } x_0 \\ \lim_{x_0} f = +\infty \end{array}\right\} \Longrightarrow \lim_{x_0} g = +\infty. \tag{ii}$$

$$\left.\begin{array}{r} g \leqslant h \textit{ dans un voisinage de } x_0 \\ \lim_{x_0} h = -\infty \end{array}\right\} \Longrightarrow \lim_{x_0} g = -\infty. \tag{iii}$$

Proposition 9.26. *$f : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$. Si* $\lim_{x_0} f = \ell \in \overline{\mathbb{R}}^*$, *alors f est du signe de ℓ dans un voisinage de x_0.*

VI Comparaison de fonctions

Définition 9.27 (o, $\mathcal{O}$ et $\sim$)**.** *$f, g : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$.*

(i) *On dit que $f = \mathcal{O}_{x_0}(g)$ lorsque $\exists K > 0$, $\exists V$ voisinage de x_0, $\forall x \in V \cap \mathcal{D}_f$, $|f(x)| \leqslant K|g(x)|$.*

(ii) *On dit que $f = o_{x_0}(g)$ lorsque $\forall \varepsilon > 0$, $\exists V$ voisinage de x_0, $\forall x \in V \cap \mathcal{D}_f$, $|f(x)| \leqslant \varepsilon|g(x)|$.*

(iii) *On dit que $f \underset{x_0}{\sim} g$ lorsque $f = g + o_{x_0}(g)$.*

Proposition 9.28. *$\underset{x_0}{\sim}$ est une relation d'équivalence. Et la relation $\mathcal{R}$ définie par $f\mathcal{R}g \Leftrightarrow f = \mathcal{O}_{x_0}(g)$ est transitive. Idem avec o.*

Proposition 9.29. *$f, g, h, k : \mathcal{D}_f \to \mathbb{R}$. x_0 adhérent à $\mathcal{D}_f$.*

$$f = o_{x_0}(g) \Longrightarrow f = \mathcal{O}_{x_0}(g). \tag{i}$$

$$\left.\begin{array}{r} f = \mathcal{O}_{x_0}(g) \\ g \underset{x_0}{\sim} h \end{array}\right\} \Longrightarrow f = \mathcal{O}_{x_0}(h). \tag{ii}$$

$$\left.\begin{array}{r} f = \mathcal{O}_{x_0}(g) \\ h = \mathcal{O}_{x_0}(g) \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} f + h = \mathcal{O}_{x_0}(g) \\ \forall \lambda \in \mathbb{R}^*,\ \lambda f = \mathcal{O}_{x_0}(g) \end{array}\right. . \tag{iii}$$

$$\left.\begin{array}{r} f \underset{x_0}{\sim} g \\ h \underset{x_0}{\sim} k \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} fh \underset{x_0}{\sim} gk \\ \frac{1}{f} \underset{x_0}{\sim} \frac{1}{g} \end{array}\right. . \tag{iv}$$

$$\left.\begin{array}{r} f \underset{x_0}{\sim} g \\ g > 0 \text{ dans un voisinage de } x_0 \end{array}\right\} \Longrightarrow f > 0 \text{ dans un voisinage de } x_0. \tag{v}$$

$$\left.\begin{array}{r} f \underset{x_0}{\sim} g \\ \lim_{x_0} g = \ell \in \overline{\mathbb{R}} \end{array}\right\} \Longrightarrow \lim_{x_0} f = \ell. \tag{vi}$$

$$\lim_{x_0} f = \ell \in \mathbb{R}^* \Longrightarrow f \underset{x_0}{\sim} \ell. \tag{vii}$$

Les propriétés (ii) *et* (iii) *restent valables en remplaçant $\mathcal{O}$ par o.*

Proposition 9.30. *$(\alpha, \beta) \in (\mathbb{R}_+^*)^2$. $a \in]1, +\infty[$.*

$$\frac{1}{1+x} = 1 - x + \mathcal{O}_0(x^2). \tag{i}$$

$$(\ln x)^\beta = o_{+\infty}\left(x^\alpha\right), \qquad x^\alpha = o_{+\infty}\left(a^x\right), \qquad a^x = o_{+\infty}\left(x^x\right). \tag{ii}$$

$$a^n = o_{+\infty}\left(n!\right), \qquad n! = o_{+\infty}\left(n^n\right). \tag{iii}$$

VII Généralités sur la continuité

Proposition 9.31. *$f : I \to \mathbb{R}$ (définie sur tout l'intervalle I). $x_0 \in I \backslash \{\inf I, \sup I\}$. f est $\mathcal{C}^0$ à droite en x_0* ssi *$\lim_{x_0^+} f$ existe et vaut $f(x_0)$. f est $\mathcal{C}^0$ à gauche en x_0* ssi *$\lim_{x_0^-} f$ existe et vaut $f(x_0)$. Et f est $\mathcal{C}^0$ en x_0* ssi *f $\mathcal{C}^0$ à droite et à gauche en x_0.*

Définition 9.32 (Prolongement par continuité)**.** *$f : I \to \mathbb{R}$ t.q. $\sup I \notin I$. Si $\lim_{\sup I} f$ existe, alors on appelle prolongement par $\mathcal{C}^0$ de f en $\sup I$ l'application*

$$x \in I \cup \{\sup I\} \longmapsto \begin{cases} f(x) \text{ si } x \neq \sup I \\ \lim_{\sup I} f \text{ sinon} \end{cases}.$$

Définition 9.33 (Prolongement par continuité)**.** *$f : I\backslash\{x_0\} \to \mathbb{R}$ t.q. x_0 intérieur à I. Si $\lim_{x_0} f$ existe, alors on appelle prolongement par $\mathcal{C}^0$ de f en x_0 l'application*

$$x \in I \longmapsto \begin{cases} f(x) \text{ si } x \neq x_0 \\ \lim_{x_0} f \text{ sinon} \end{cases}.$$

Proposition 9.34. *$f : I \to \mathbb{R}$. Si pour toute suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de I convergeant vers x_0, $f(u_n) \xrightarrow[n\to+\infty]{} f(x_0)$, alors f est $\mathcal{C}^0$ en $x_0 \in I$.*

Proposition 9.35. *$f, g : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I. $A \subset I$ t.q. tout point de I est limite d'une suite de points de A. Si $f = g$ sur A, alors $f = g$ sur I.*

Proposition 9.36. *$f, g : I \to \mathbb{R}$ $\mathcal{C}^0$ en $x_0 \in I$ (resp. sur I). Les fonctions $|f|, \max(f,g), \min(f,g), (f+g), (fg), \left(\frac{f}{g}\right)$ (si $g(x_0) \neq 0$) sont $\mathcal{C}^0$ en x_0 (resp. sur I).*

Définition 9.37 (Fonction lipschitzienne)**.** *$f : I \to \mathbb{R}$ est dite* lipschitzienne *sur I de rapport $k > 0$ lorsque*

$$\forall (x,y) \in I^2,\ |f(x) - f(y)| \leqslant k|x - y|.$$

Définition 9.38 (Fonction contractante)**.** *Une fonction est dite* contractante *si elle est lipschitzienne de rapport strictement inférieur à 1.*

Proposition 9.39. *Toute fonction lipschitzienne sur I est $\mathcal{C}^0$ sur I.*

VIII Théorème de la limite monotone

Théorème 9.40 (Théorème de la limite monotone)**.** *$f :]a,b[\to \mathbb{R}$, $a < b$ réels ou non. $f \nearrow$ sur $]a,b[$.*

(i) *Si f majorée alors $\lim_{b^-} f$ existe et vaut $\sup_{x\in]a,b[} f(x)$.*

(ii) *Si f non majorée alors $\lim_{b^-} f = +\infty$.*

(iii) *Si f minorée alors $\lim_{a^+} f$ existe et vaut $\inf_{x\in]a,b[} f(x)$.*

(iv) *Si f non minorée alors $\lim_{a^+} f = -\infty$.*

Idem si $f \searrow$.

Corollaire 9.41. *$f : I \to \mathbb{R}$ monotone sur I intervalle. Alors f admet une limite à droite et à gauche en tout point intérieur à I. De plus, si $f \nearrow$ sur I, on a :*

$$\forall x_0 \in I,\ \lim_{x_0^-} f \leqslant f(x_0) \leqslant \lim_{x_0^+} f, \tag{i}$$

$$\forall (x_0, x_1) \in I^2,\ x_0 < x_1 \Longrightarrow \lim_{x_0^+} f \leqslant \lim_{(x_1)^-} f. \tag{ii}$$

Idem si $f \searrow$.

IX Quelques théorèmes importants

IX.1 Théorème des valeurs intermédiaires

Théorème 9.42 (Théorème des valeurs intermédiaires)**.** *L'image d'un intervalle I par une application $\mathcal{C}^0$ sur I est un intervalle. Autrement dit, soit $f : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I intervalle, alors*

$$\forall (a,b) \in I^2,\ \forall \gamma \in [f(a), f(b)],\ \exists c \in [a,b],\ \gamma = f(c).$$

Démonstration. Construction par *dichotomie*. Soit $(a,b) \in I^2$, $f(a) < f(b)$, $\gamma \in]f(a), f(b)[$. Construire deux suites adjacentes $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ telles que $\forall n \in \mathbb{N}$, $f(a_n) \leqslant \gamma \leqslant f(b_n)$. Poser $a_0 = a$, $b_0 = b$, puis, après avoir construit $a_0 \leqslant \cdots \leqslant a_n \leqslant b_n \leqslant \cdots \leqslant b_0$, procéder comme suit : si $\gamma \leqslant f\left(\frac{a_n+b_n}{2}\right)$, poser $a_{n+1} = a_n$ et $b_{n+1} = \frac{a_n+b_n}{2}$; sinon, poser $a_{n+1} = \frac{a_n+b_n}{2}$, $b_{n+1} = b_n$. Vérifier que $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont adjacentes, et en déduire qu'elles convergent vers une même limite $c \in [a,b]$. En utilisant la continuité de f, obtenir $\gamma = f(c)$. □

Corollaire 9.43. *$f : [a, +\infty[\to \mathbb{R}$ $\mathcal{C}^0$ sur $[a, +\infty[$ et $\lim_{+\infty} f = \ell \in \overline{\mathbb{R}}$.*

$$\forall \gamma \in [f(a), \ell[,\ \exists c \in [a, +\infty[,\ \gamma = f(c).$$

Corollaire 9.44. *$f : [a, b[\to \mathbb{R}$ $\mathcal{C}^0$ sur $[a, b[$, $a < b$, $f \nearrow\nearrow$ sur $[a, b[$.*

$$f([a, b[) = \left[f(a), \lim_{b^-} f \right[.$$

IX.2 Image d'un segment

Lemme 9.45. *Soit $X \subset \mathbb{R}$, $X \neq \varnothing$.*

$$\exists (x_n) \in X^{\mathbb{N}},\ x_n \xrightarrow[n\to+\infty]{} \sup X.$$

Théorème 9.46. *L'image d'un segment S par une application $\mathcal{C}^0$ sur S est un segment.*

Démonstration. Soit f $\mathcal{C}^0$ sur $[a,b]$, $X = f([a,b])$. *Première étape* : montrer que X est borné. Pour cela, raisonner par l'absurde et supposer X non majoré. Alors par le lemme 9.45, $\exists (c_n) \in [a,b]^{\mathbb{N}}$, $f(c_n) \xrightarrow[n\to+\infty]{} +\infty$. Comme $(c_n)_{n\in\mathbb{N}}$ est bornée, utiliser Bolzano-Weierstrass (théorème 8.56) pour obtenir $c_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell \in [a,b]$, et $f(c_{\varphi(n)}) \xrightarrow[n\to+\infty]{} f(\ell) \in X$ (par la $\mathcal{C}^0$ de f). Contradiction, donc X est majoré. De même, X est minoré. *Deuxième étape* : montrer que $\sup X$ et $\inf X$ sont atteints par f. Par le lemme 9.45, $\exists (d_n) \in [a,b]^{\mathbb{N}}$, $f(d_n) \xrightarrow[n\to+\infty]{} \sup X$. Comme $(d_n)_{n\in\mathbb{N}}$ est bornée, utiliser Bolzano-Weierstrass (théorème 8.56) pour obtenir $d_{\psi(n)} \xrightarrow[n\to+\infty]{} \varpi \in [a,b]$, et $f(d_{\psi(n)}) \xrightarrow[n\to+\infty]{} f(\varpi) \in X$ (par la $\mathcal{C}^0$ de f). Donc $\sup X = f(\varpi)$. De même avec $\inf X$. Au final, X est un intervalle (par le théorème 9.42) et $\sup X \in X$, $\inf X \in X$, donc X est un segment. □

IX.3 Continuité et injectivité

Vocabulaire 9.47 (Homéomorphisme)**.** *Une fonction f $\mathcal{C}^0$ et bijective de I sur J est dite* homéomorphisme *lorsque f^{-1} est $\mathcal{C}^0$ sur J.*

Théorème 9.48. *$f : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I intervalle.*

$$f \text{ injective sur } I \Longrightarrow f \text{ strictement monotone sur } I.$$

Démonstration. Soit $(a,b) \in I^2$, $a < b$. On suppose $f(a) < f(b)$. Soit $(x,y) \in I^2$, $x < y$. Poser $\phi : t \in [0,1] \longmapsto f(ta + (1-t)x) - f(tb + (1-t)y)$. Raisonner par l'absurde pour montrer que ϕ ne s'annule pas sur $[0,1]$ (si $\phi(t_0) = 0$, on aurait $f(t_0 a + (1-t_0)x) = f(t_0 b + (1-t_0)y)$, donc par l'injectivité de f, $t_0(b-a) + (1-t_0)(y-x) = 0$). Donc ϕ est de signe constant sur $[0,1]$. Or $\phi(1) < 0$, donc $\phi(0) < 0$, donc $f(x) < f(y)$. D'où $f \nearrow\nearrow$. □

Lemme 9.49. *$g : J \to \mathbb{R}$ strictement monotone sur J intervalle et $g(J)$ est un intervalle. Alors g est $\mathcal{C}^0$ sur J.*

Démonstration. On suppose $g \nearrow\nearrow$ sur J. Par l'absurde, supposer qu'il existe $x_0 \in J \backslash \{\sup J\}$ tel que g n'est pas $\mathcal{C}^0$ à droite en x_0. Comme $g \nearrow$, $\lim_{x_0^+} g = \inf_{x > x_0} g(x)$. Or g non $\mathcal{C}^0$ à droite en x_0 donc $g(x_0) < \lim_{x_0^+} g$. Donc $]g(x_0), \lim_{x_0^+} g[\cap g(J) = \varnothing$. Soit $x_1 \in]x_0, \sup J[$, alors $\lim_{x_0^+} g \leqslant g(x_1)$, donc $]g(x_0), \lim_{x_0^+} g[\subset [g(x_0), g(x_1)] \subset g(J)$. Donc $]g(x_0), \lim_{x_0^+} g[= \varnothing$. Contradiction. Raisonner de même pour la continuité à gauche. □

Théorème 9.50. *$f : I \to \mathbb{R}$ $\mathcal{C}^0$ et bijective de I sur $f(I)$. Alors f^{-1} est $\mathcal{C}^0$ sur $f(I)$.*

IX.4 Théorème du point fixe

Théorème 9.51 (Théorème du point fixe)**.** *$f : I \to \mathbb{R}$ contractante, où I est un intervalle fermé, $f(I) \subset I$. Alors la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 \in I$ et $\forall n \in \mathbb{N}$, $u_{n+1} = f(u_n)$ converge vers l'unique point fixe de f sur I.*

Démonstration. Soit $n \in \mathbb{N}^*$, $p \in \mathbb{N}^*$. *Première étape* : majorer $|u_{n+p} - u_n|$. Pour cela, écrire $|u_{n+1} - u_n| = |f(u_n) - f(u_{n-1})| \leqslant k|u_n - u_{n-1}|$, en déduire par récurrence que $|u_{n+1} - u_n| \leqslant k^n |u_1 - u_0|$. Obtenir alors

$$|u_{n+p} - u_n| = \left| \sum_{i=n}^{n+p-1} (u_{i+1} - u_i) \right| \leqslant \sum_{i=n}^{n+p-1} |u_{i+1} - u_i| \leqslant k^n \frac{|u_1 - u_0|}{1-k}. \qquad (*)$$

Deuxième étape : montrer que f a un unique point fixe. Soit $(\ell, \ell') \in I^2$, tels que $f(\ell) = \ell$, $f(\ell') = \ell'$. Alors $|\ell - \ell'| = |f(\ell) - f(\ell')| \leqslant k|\ell - \ell'|$, donc $\ell = \ell'$. *Troisième étape* : montrer que toute valeur d'adhérence de $(u_n)_{n\in\mathbb{N}}$ est un point fixe de f. Par $(*)$, il vient $|u_p - u_0| \leqslant \frac{|u_1 - u_0|}{1-k}$. Donc $(u_n)_{n\in\mathbb{N}}$ bornée. Soit α une valeur d'adhérence de $(u_n)_{n\in\mathbb{N}}$; on note $\varphi : \mathbb{N} \to \mathbb{N} \nearrow\nearrow$ t.q. $u_{\varphi(n)} \xrightarrow[n\to+\infty]{} \alpha$. On a $f(u_{\varphi(n)}) = u_{\varphi(n)+1}$, donc $u_{\varphi(n)+1} \xrightarrow[n\to+\infty]{} f(\alpha)$. Or $u_{\varphi(n)+1} - u_{\varphi(n)} \xrightarrow[n\to+\infty]{} 0$. Donc $\alpha = f(\alpha)$. Donc $(u_n)_{n\in\mathbb{N}}$ admet une unique valeur d'adhérence α ; ainsi $u_n \xrightarrow[n\to+\infty]{} \alpha$. □

Chapitre 10

Dérivabilité

Notation 10.1. *Dans toute la suite, I et J sont des intervalles de $\mathbb{R}$ non vides et non réduits à un point.*

Notation 10.2. *On note $\mathring{I} = I\backslash\{\inf I, \sup I\}$.*

I Généralités

I.1 Définition

Définition 10.3 (Dérivabilité)**.** *$f : I \to \mathbb{R}$. $x_0 \in I$. On note*

$$\tau_{x_0} : x \in I\backslash\{x_0\} \longmapsto \frac{f(x) - f(x_0)}{x - x_0}.$$

(i) *On dit que f est* dérivable *en x_0 lorsque τ_{x_0} a une limite finie en x_0. Dans ce cas, on note $f'(x_0) = \lim_{x_0} \tau_{x_0}$.*

(ii) *On dit que f est* dérivable à droite *(resp.* à gauche*) en x_0 lorsque τ_{x_0} a une limite finie à droite (resp. à gauche) en x_0. On note $f'_d(x_0) = \lim_{x_0^+} \tau_{x_0}$ (resp. $f'_g(x_0) = \lim_{x_0^-} \tau_{x_0}$).*

(iii) *On dit que f est* dérivable sur *I lorsque f est dérivable en tout point de $\mathring{I}$, et f est dérivable à droite en $\inf I$, à gauche en $\sup I$. On appelle dans ce cas f' l'*application dérivée *de f définie par $f' : x \in I \longmapsto f'(x)$.*

Vocabulaire 10.4. *$f : I \to \mathbb{R}$, $J \subsetneq I$. Alors f dérivable sur J signifie $f_{|J}$ dérivable.*

Proposition 10.5 (Caractérisation de la dérivabilité)**.** *$f : I \to \mathbb{R}$, x_0 intérieur à I. f est dérivable en x_0* ssi *f est dérivable à droite et à gauche en x_0 et $f'_g(x_0) = f'_d(x_0)$.*

Proposition 10.6 (Définition équivalente de la dérivabilité)**.** *$f : I \to \mathbb{R}$. $x_0 \in I$. f est dérivable en x_0* ssi

$$\exists \varrho \in \mathbb{R},\ f(x) = f(x_0) + (x - x_0)\varrho + o_{x_0}(x - x_0).$$

Dans ce cas, on note $f'(x_0) = \varrho$.

Vocabulaire 10.7 (Développement limité)**.** *On dit que f admet un $DL_n(x_0)$ (*développement limité *en x_0 à l'ordre n) lorsque*

$$\exists (a_0, \ldots, a_n) \in \mathbb{R}^{n+1},\ f(x) = \left(\sum_{k=0}^{n} a_k (x - x_0)^k\right) + o_{x_0}\left((x - x_0)^n\right).$$

Proposition 10.8. *$f : I \to \mathbb{R}$. $x_0 \in I$. Si f dérivable en x_0, alors f $\mathcal{C}^0$ en x_0.*

Proposition 10.9. *$f : I \to \mathbb{R}$. $x_0 \in I$. f dérivable en x_0* ssi *f admet un $DL_1(x_0)$.*

Corollaire 10.10.

$$\ln(1+x) \underset{0}{\sim} x, \qquad e^x - 1 \underset{0}{\sim} x, \qquad (1+x)^\alpha - 1 \underset{0}{\sim} \alpha x,$$

$$\sin x \underset{0}{\sim} x, \qquad \tan x \underset{0}{\sim} x, \qquad \cos x - 1 \underset{0}{\sim} -\frac{x^2}{2}.$$

Définition 10.11 (Tangente)**.** *$f : I \to \mathbb{R}$ dérivable en $x_0 \in I$. On appelle tangente à la courbe représentative de f la droite d'équation*

$$y = f(x_0) + (x - x_0)f'(x_0).$$

I.2 Opérations et dérivation

Proposition 10.12. *$f, g : I \to \mathbb{R}$ dérivables en $x_0 \in I$. Alors :*

$$(f+g) \text{ dérivable en } x_0 \text{ et } (f+g)'(x_0) = f'(x_0) + g'(x_0), \tag{i}$$

$$(fg) \text{ dérivable en } x_0 \text{ et } (fg)'(x_0) = f'(x_0)g(x_0) + f(x_0)g'(x_0), \tag{ii}$$

$$\left(\frac{1}{f}\right) \text{ dérivable en } x_0 \text{ si } f(x_0) \neq 0 \text{ et } \left(\frac{1}{f}\right)'(x_0) = -\frac{f'(x_0)}{(f(x_0))^2}. \tag{iii}$$

Démonstration. Utiliser la proposition 10.6. □

Corollaire 10.13. *$f : I \to \mathbb{R}$ dérivable en $x_0 \in I$. $n \in \mathbb{N}^*$. Alors $f^n = f \cdot f \cdots f$ est dérivable en x_0 et $(f^n)'(x_0) = nf'(x_0)f^{n-1}(x_0)$.*

I.3 Composition et dérivation

Proposition 10.14. *$f : I \to \mathbb{R}$ dérivable en $x_0 \in I$, $g : J \to \mathbb{R}$ dérivable en $f(x_0)$, avec $J \supset f(I)$. Alors $(g \circ f)$ est dérivable en x_0 et*

$$(g \circ f)'(x_0) = g'(f(x_0))f'(x_0).$$

I.4 Dérivée d'une fonction réciproque

Proposition 10.15. *$f : I \to \mathbb{R}$ $\mathcal{C}^0$ et strictement monotone sur I. f dérivable en $x_0 \in I$. Alors f^{-1} est dérivable en $f(x_0)$* ssi *$f'(x_0) \neq 0$.*

Démonstration. ($\Rightarrow$) Clair. ($\Leftarrow$) Poser $\Delta_h = f^{-1}(f(x_0) + h) - f^{-1}(f(x_0))$. Utiliser $\Delta_h = o_0(1)$ et $f^{-1}(f(x_0) + h) = x_0 + \Delta_h$ pour en déduire que $f(x_0) + h = f(x_0 + \Delta_h) = f(x_0) + \Delta_h f'(x_0) + o_0(\Delta_h)$, d'où $h = \Delta_h(f'(x_0) + o_0(1))$ donc $\frac{\Delta_h}{h} \underset{0}{\sim} \frac{1}{f'(x_0)}$. □

Corollaire 10.16. *$f : I \to \mathbb{R}$ $\mathcal{C}^k$ sur I, $k \in \mathbb{N}^*$, f strictement monotone sur I, f' ne s'annule pas sur I, alors f^{-1} $\mathcal{C}^k$ sur $f(I)$.*

I.5 Dérivation des fonctions usuelles

Proposition 10.17. *Les fonctions polynomiales sont $\mathcal{C}^\infty$ sur $\mathbb{R}$, les fractions rationnelles sont $\mathcal{C}^\infty$ sur leurs ensembles de définition,* ln *est $\mathcal{C}^\infty$ sur $\mathbb{R}_+^*$,* exp, sin *et* cos *sont $\mathcal{C}^\infty$ sur $\mathbb{R}$.*

II Théorème de Rolle et accroissements finis

II.1 Condition nécessaire d'extremum

Théorème 10.18 (Condition nécessaire d'extremum)**.** *$f : I \to \mathbb{R}$ dérivable en $a \in \mathring{I}$. Si f a un extremum local en a alors $f'(a) = 0$.*

Démonstration. Montrer que, pour h suffisamment proche de 0, $\frac{f(a+h)-f(a)}{h} \geqslant 0$ avec $h > 0$ et $\frac{f(a+h)-f(a)}{h} \leqslant 0$ avec $h < 0$. En déduire que $f'(a) \geqslant 0$ et $f'(a) \leqslant 0$. □

Vocabulaire 10.19. *Un point a pour lequel $f'(a) = 0$ est dit* point critique.

II.2 Théorème de Rolle

Théorème 10.20 (Théorème de Rolle)**.** *$f : [a, b] \to \mathbb{R}$ $\mathcal{C}^0$ sur $[a, b]$ et dérivable sur $]a, b[$ avec $f(a) = f(b)$.*

$$\exists c \in]a, b[,\ f'(c) = 0.$$

Démonstration. Conséquence du théorème 10.18. □

II.3 Théorème des accroissements finis

Théorème 10.21 (Théorème des accroissements finis)**.** *$f : [a, b] \to \mathbb{R}$ $\mathcal{C}^0$ sur $[a, b]$ et dérivable sur $]a, b[$.*

$$\exists c \in]a, b[,\ f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Autrement dit : $\exists \lambda \in]0, 1[,\ f(b) - f(a) = (b - a)f'(\lambda a + (1 - \lambda)b)$.

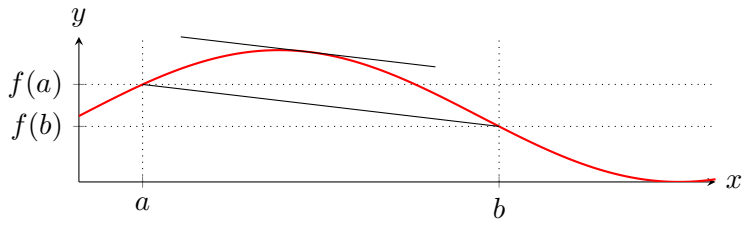


Illustration du théorème des accroissements finis

Démonstration. Poser $g : x \in [a, b] \longmapsto f(x) - x\frac{f(b)-f(a)}{b-a}$. Appliquer alors le théorème de Rolle (théorème 10.20) à g et en déduire le résultat souhaité. □

Corollaire 10.22 (Inégalité des accroissements finis)**.** *$f : [a, b] \to \mathbb{R}$ $\mathcal{C}^0$ sur $[a, b]$ et dérivable sur $]a, b[$. Si $\forall x \in]a, b[,\ m \leqslant f'(x) \leqslant M$, alors*

$$m(b - a) \leqslant f(b) - f(a) \leqslant M(b - a).$$

Corollaire 10.23 (Caractérisation des fonctions lipschitziennes)**.** *$f : I \to \mathbb{R}$ dérivable sur I. Alors f' est bornée sur I* ssi *f est lipschitzienne sur I.*

Corollaire 10.24. *Si $f : [a, b] \to \mathbb{R}$ est $\mathcal{C}^1$ sur $[a, b]$, alors f est lipschitzienne sur $[a, b]$.*

II.4 Monotonie et dérivée

Théorème 10.25. *$f : I \to \mathbb{R}$ $\mathcal{C}^0$ sur $\mathring{I}$.*

(i) *$f' \geqslant 0$ sur $\mathring{I} \iff f \nearrow$ sur I,*

(ii) *$f' = 0$ sur $\mathring{I} \iff f$ constante sur I,*

(iii) *$f' > 0$ sur $\mathring{I}$ excepté en un nombre fini de points $\implies f \nearrow\!\!\nearrow$ sur I.*

Corollaire 10.26. *$f, g : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I et dérivables sur $\mathring{I}$. $(a, b) \in I^2$, $a < b$.*

$$f' \leqslant g' \implies f(b) - f(a) \leqslant g(b) - g(a).$$

Proposition 10.27. *$f : I \to \mathbb{R}$ dérivable sur I, $a \in I$, $n \in \mathbb{N}$.*

$$f'(x) = \mathcal{O}_a\left((x-a)^n\right) \implies f(x) - f(a) = \mathcal{O}_a\left((x-a)^{n+1}\right).$$

Cette propriété reste valable en remplaçant $\mathcal{O}$ par o.

III Limites et dérivée

Théorème 10.28 (Théorème de la limite de la dérivée)**.** *$f : I \to \mathbb{R}$ $\mathcal{C}^0$ sur I et dérivable sur $I\backslash\{a\}$. Si $\lim_a f' = \ell \in \mathbb{R}$ alors f est dérivable en a et $f'(a) = \ell$.*

Démonstration. Soit $x \in I\backslash\{a\}$. Utiliser le théorème des accroissements finis (théorème 10.21) pour montrer que $\exists c \in]a, x[$, $f'(c) = \frac{f(x)-f(a)}{x-a}$. Soit $\varepsilon > 0$, alors $\exists \eta > 0$, $\forall x \in]a-\eta, a+\eta[\backslash\{a\} \cap I$, $|f'(x) - \ell| \leqslant \varepsilon$. En choisissant x tel que $0 < |x-a| < \eta$, on a $\left|\frac{f(x)-f(a)}{x-a} - \ell\right| \leqslant \varepsilon$, d'où $f'(a) = \ell$. □

Théorème 10.29. *$f : I\backslash\{a\} \to \mathbb{R}$ $\mathcal{C}^k$ sur $I\backslash\{a\}$ et $\forall i \in [\![0, k]\!]$, $\lim_a f^{(i)} = \ell_i \in \mathbb{R}$. Alors le prolongement par $\mathcal{C}^0$ f_0 de f en a existe, est $\mathcal{C}^k$ sur I et $\forall i \in [\![0, k]\!]$, $f_0^{(i)}(a) = \ell_i$.*

Démonstration. Par récurrence en utilisant le théorème 10.28. □

Chapitre 11

Fonctions à Valeurs Complexes

Notation 11.1. *Dans toute la suite, I est un intervalle non vide de $\mathbb{R}$ et a est un point adhérent à I.*

I Limites, continuité, dérivabilité

Définition 11.2 (Limite)**.** *$f : I \to \mathbb{C}$. On dit que $\lim_a f = \ell \in \mathbb{C}$ lorsque $\lim_{x\to a} |f(x) - \ell| = 0$. Si de plus $f(a) = \ell$, on dit que f est $\mathcal{C}^0$ en a.*

Définition 11.3 (Dérivabilité)**.** *$f : I \to \mathbb{C}$. On dit que f est* dérivable *en a lorsque le taux d'accroissement τ_a (voir définition 10.3) admet une limite complexe finie en a.*

Remarque 11.4. *On définit alors la continuité et la dérivabilité sur I, les dérivées n-ièmes, les fonctions de classes $\mathcal{C}^n$ et $\mathcal{C}^\infty$ exactement comme pour les fonctions à valeurs réelles.*

Proposition 11.5. *$f : I \to \mathbb{C}$.*

$$\lim_a f = \ell \iff \begin{cases} \lim_a \Re(f) = \Re(\ell) \\ \lim_a \Im(f) = \Im(\ell) \end{cases} . \tag{i}$$

$$f \text{ dérivable en } a \iff \begin{cases} \Re(f) \text{ dérivable en } a \\ \Im(f) \text{ dérivable en } a \end{cases}$$

$$\text{et dans ce cas } \begin{cases} \Re(f') = (\Re(f))' \\ \Im(f') = (\Im(f))' \end{cases} . \tag{ii}$$

$$f \ \mathcal{C}^n \text{ sur } I \iff \begin{cases} \Re(f) \ \mathcal{C}^n \text{ sur } I \\ \Im(f) \ \mathcal{C}^n \text{ sur } I \end{cases} . \tag{iii}$$

$$f \ \mathcal{C}^0 \text{ sur } I \implies \begin{cases} |f| \ \mathcal{C}^0 \text{ sur } I \\ \overline{f} \ \mathcal{C}^0 \text{ sur } I \end{cases} . \tag{iv}$$

II Opérations usuelles

Proposition 11.6. *La somme, le produit, le quotient (si le dénominateur ne s'annule pas), la composée de fonctions de classe $\mathcal{C}^n$ (resp. dérivables) sont de classe $\mathcal{C}^n$ (resp. dérivables).*

Proposition 11.7. *La formule de Leibniz (voir théorème 5.28) et la formule de dérivation d'une composée (voir proposition 10.14) sont encore vraies.*

III Les théorèmes

Proposition 11.8. *Pour toute fonction f continue sur un segment $[a,b]$, $|f|$ est bornée et atteint ses bornes sur $[a,b]$ (voir théorème 9.46).*

Proposition 11.9. *Pour toute fonction f dérivable sur I, f est constante sur I* ssi *$f'=0$ sur I.*

Remarque 11.10. *Pour les fonctions à valeurs complexes, le théorème de Rolle (théorème 10.20) est faux, donc le théorème des accroissements finis (théorème 10.21) aussi. Cependant, l'inégalité des accroissements finis (corollaire 10.22) reste vraie.*

Théorème 11.11 (Inégalité des accroissements finis)**.** *$f:[a,b]\to\mathbb{C}$ $\mathcal{C}^0$ sur $[a,b]$ et $\mathcal{C}^1$ sur $]a,b[$. Si $\forall x\in]a,b[$, $|f'(x)|\leqslant\lambda$, alors*

$$|f(b)-f(a)|\leqslant\lambda|b-a|.$$

Corollaire 11.12. *$f:I\to\mathbb{C}$ $\mathcal{C}^0$ sur I et $\mathcal{C}^1$ sur $\mathring{I}$. $k\in\mathbb{R}_+$. Alors f est k-lipschitzienne sur I* ssi *$\forall x\in\mathring{I}$, $|f'(x)|\leqslant k$.*

Théorème 11.13 (Prolongement d'une application $\mathcal{C}^1$)**.** *$f:I\to\mathbb{C}$ $\mathcal{C}^0$ sur I, $\mathcal{C}^1$ sur $I\backslash\{a\}$, et avec $\lim_a f'=\ell\in\mathbb{C}$. Alors f est $\mathcal{C}^1$ sur I et $f'(a)=\ell$.*

Démonstration. Définir l'application $F:I\to\mathbb{C}$ par $\forall x\in I\backslash\{a\}$, $F(x)=f'(x)$ et $F(a)=\ell$. F est $\mathcal{C}^0$ sur I donc admet une primitive g sur I telle que $g(a)=f(a)$. Et $\forall x\in I\cap]-\infty,a[$, $g'(x)=F(x)=f'(x)$ donc $(g-f)$ est constante sur $I\cap]-\infty,a[$. De même, $(g-f)$ est constante sur $I\cap]a,+\infty[$. Or $(g-f)$ est $\mathcal{C}^0$ en a donc $\lim_a(g-f)=g(a)-f(a)=0$. Donc $\forall x\in I$, $g(x)=f(x)$. Ainsi $f=g$ est de classe $\mathcal{C}^1$ en tant que primitive d'une application $\mathcal{C}^0$. □

Corollaire 11.14. *$f:I\to\mathbb{C}$ $\mathcal{C}^0$ sur I, $\mathcal{C}^k$ sur $I\backslash\{a\}$. $k\in\mathbb{N}\cup\{\infty\}$. On suppose que*

$$\forall h\in[\![1,k]\!]\cap\mathbb{N},\ \exists\ell_h\in\mathbb{C},\ \lim_a f^{(h)}=\ell_h.$$

Alors f est $\mathcal{C}^k$ sur I.

Démonstration. Par récurrence à l'aide du théorème 11.13. □

Chapitre 12

Développements Limités

I Approximation de fonctions par des fonctions polynomiales

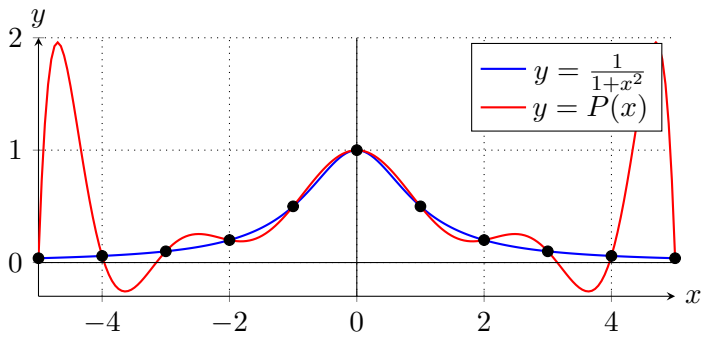
I.1 Point de vue global

Proposition 12.1. *$f : [a,b] \to \mathbb{R}$ $\mathcal{C}^{n+1}$ sur $[a,b]$. $a \leqslant x_0 < \cdots < x_n \leqslant b$. On définit le* polynôme d'interpolation de Lagrange *de f en $x_0, \ldots, x_n$ par*

$$P : x \in [a,b] \longmapsto \sum_{i=0}^{n} \left(f(x_i) \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)} \right).$$

Alors

$$\forall x \in [a,b],\ |f(x) - P(x)| \leqslant \sup_{[a,b]} \left| f^{(n+1)} \right| \cdot \frac{(b-a)^{n+1}}{(n+1)!}.$$



Une fonction et son polynôme interpolateur

Démonstration. Soit $A \in \mathbb{R}$, $\psi : x \in [a,b] \longmapsto f(x) - P(x) - A\prod_{i=0}^{n}(x - x_i)$, $t \in [a,b] \backslash \{x_0, \ldots, x_n\}$. Choisir A t.q. $\psi(t) = 0$. On a ψ $\mathcal{C}^{n+1}$ sur $[a,b]$ et $\psi(x_0) = \cdots = \psi(x_n) = \psi(t) = 0$, donc ψ s'annule en $(n+2)$ points deux à deux distincts. En itérant le théorème de Rolle (théorème 10.20), en déduire que $\psi^{(n+1)}$ s'annule en au moins un point $c \in [a,b]$. Or $\psi^{(n+1)} = f^{(n+1)} - (n+1)!A$, donc $A = \frac{f^{(n+1)}(c)}{(n+1)!}$. Comme $\psi(t) = 0$, il vient $f(t) - P(t) = \frac{f^{(n+1)}(c)}{(n+1)!} \prod_{i=0}^{n}(t - x_i)$. Donc $\forall t \in [a,b]$, $|f(t) - P(t)| \leqslant \frac{\sup_{[a,b]} \left| f^{(n+1)} \right|}{(n+1)!} \prod_{i=0}^{n} |t - x_i| \leqslant \frac{\sup_{[a,b]} \left| f^{(n+1)} \right|}{(n+1)!} (b-a)^{n+1}$. □

I.2 Point de vue local

Proposition 12.2. *$f : [a,b] \to \mathbb{R}$ $\mathcal{C}^p$ sur $[a,b]$, $x_0 \in [a,b]$. Alors il existe au moins une fonction polynomiale $\mathcal{T}_{p,f,x} \in \mathbb{R}^{\mathbb{R}}$ vérifiant $\forall k \in [\![0,p]\!]$, $\mathcal{T}_{p,f,x}^{(k)}(x_0) = f^{(k)}(x_0)$ et donnée par*

$$\mathcal{T}_{p,f,x} : x \in \mathbb{R} \longmapsto \sum_{k=0}^{p} \frac{f^k(x_0)}{k!}(x-x_0)^k.$$

$\mathcal{T}_{p,f,x}$ est dit polynôme de Taylor *de f en x_0 de degré p, et est parfois noté simplement $\mathcal{T}_p$.*

Remarque 12.3. *Si f est paire alors*

$$\forall x \in \mathbb{R},\ \mathcal{T}_{2p,f,0}(x) = \sum_{k=0}^{p} \frac{f^{(2k)}(0)}{(2k)!}x^{2k}.$$

Si f est impaire alors

$$\forall x \in \mathbb{R},\ \mathcal{T}_{2p+1,f,0}(x) = \sum_{k=0}^{p} \frac{f^{(2k+1)}(0)}{(2k+1)!}x^{2k+1}.$$

II Formule de Taylor

Proposition 12.4 (Formule de Taylor avec reste intégral)**.** *$f : I \to \mathbb{K}$ $\mathcal{C}^{p+1}$ sur I, $(a,x) \in I^2$.*

$$f(x) = \underbrace{\sum_{k=0}^{p} \frac{f^k(a)}{k!}(x-a)^k}_{\mathcal{T}_{p,f,a}(x)} + \underbrace{\int_a^x \frac{f^{(p+1)}(t)}{p!}(x-t)^p \,\mathrm{d}t}_{R_{p,f,a}(x)}.$$

On peut aussi écrire cette formule comme suit ($h \in \mathbb{R}$ t.q. $(a+h) \in I$) :

$$f(a+h) = \sum_{k=0}^{p} \frac{f^{(k)}(a)}{k!}h^k + \frac{h^{p+1}}{p!}\int_0^1 (1-\lambda)^p f^{(p+1)}(a+\lambda h)\,\mathrm{d}\lambda.$$

Démonstration. Par récurrence en utilisant l'intégration par parties (proposition 7.7). □

Corollaire 12.5. *$\mathcal{Q} : \mathbb{R} \to \mathbb{R}$ une fonction polynomiale de degré inférieur ou égal à p. Alors $\forall a \in \mathbb{R}$, $\mathcal{T}_{p,\mathcal{Q},a} = \mathcal{Q}$.*

III Inégalité de Taylor-Lagrange

Proposition 12.6 (Inégalité de Taylor-Lagrange)**.** *$f : I \to \mathbb{K}$ $\mathcal{C}^{p+1}$ sur I, $(a,x) \in I^2$.*

$$|f(x) - \mathcal{T}_{p,f,a}(x)| \leqslant \sup_{[a,x]} \left|f^{(p+1)}\right| \cdot \frac{|x-a|^{p+1}}{(p+1)!}.$$

Corollaire 12.7. *$f : I \to \mathbb{K}$ $\mathcal{C}^{p+1}$ dans un voisinage de $a \in \mathbb{R}$.*

$$f(x) = \mathcal{T}_{p,f,a}(x) + \mathcal{O}_a\left((x-a)^{p+1}\right).$$

IV Formule de Taylor-Young

Proposition 12.8 (Formule de Taylor-Young)**.** *$f : I \to \mathbb{K}$ $\mathcal{C}^p$ dans un voisinage de $a \in \mathbb{R}$.*

$$f(x) = \mathcal{T}_{p,f,a}(x) + o_a\left((x-a)^p\right).$$

Démonstration. *Première étape* : $\mathbb{K} = \mathbb{R}$. Appliquer la formule de Taylor avec reste intégral (proposition 12.4) en remplaçant p par $(p-1)$, car f est $\mathcal{C}^p$. Ainsi $f(x) = \mathcal{T}_{p-1,f,a}(x) + R_{p-1,f,a}(x)$. Montrer qu'il existe $c \in I$ t.q. $R_{p-1,f,a}(x) = \frac{f^{(p)}(c)}{p!}(x-a)^p$. Pour cela, $f^{(p)}$ est $\mathcal{C}^0$ sur $[a,x]$ donc bornée et atteint ses bornes : $m_p = \inf_{[a,x]} f^{(p)}$, $M_p = \sup_{[a,x]} f^{(p)}$. Si $x > a$, on obtient $m_p \leqslant R_{p-1,f,a}(x)\frac{p!}{(x-a)^p} \leqslant M_p$; si $x < a$, on a $m_p \leqslant (-1)^p R_{p-1,f,a}(x)\frac{p!}{(x-a)^p} \leqslant M_p$. Or m_p et M_p sont atteints par $f^{(p)}$ qui est $\mathcal{C}^0$ sur $[a,x]$ donc $\exists c \in [a,x]$, $f^{(p)}(c) = R_{p-1,f,a}(x)\frac{p!}{(x-a)^p}$. Le résultat voulu découle du fait que $f^{(p)}(c) = f^{(p)}(a) + o_a(1)$ (car $f^{(p)}$ $\mathcal{C}^0$ en a). *Deuxième étape* : $\mathbb{K} = \mathbb{C}$. Se ramener à la partie réelle et à la partie imaginaire. □

V Formule de Taylor-Lagrange

Corollaire 12.9 (Formule de Taylor-Lagrange)**.** *$f : I \to \mathbb{K}$ $\mathcal{C}^p$ sur I. $(a,x) \in I^2$.*

$$\exists c \in [a,x],\ f(x) = \mathcal{T}_{p-1,f,a}(x) + \frac{(x-a)^p}{p!} f^{(p)}(c).$$

VI Développements limités

VI.1 Généralités

Définition 12.10 (Développement limité)**.** *$f : I \to \mathbb{K}$. $a \in I$. On dit que f admet un $DL_p(a)$ (*développement limité *en a à l'ordre p) lorsque*

$$\exists (\alpha_0, \ldots, \alpha_p) \in \mathbb{K}^{p+1},\ f(x) = \underbrace{\sum_{k=0}^{p} \alpha_k (x-a)^k}_{\text{partie principale du } DL} + o_a\left((x-a)^p\right).$$

Notation 12.11. *Lorsque la partie principale du DL est non nulle, on utilisera plutôt l'*écriture normalisée *:*

$$f(a+h) = \alpha_s h^s \left(\sum_{k=0}^{p-s} \frac{\alpha_{k+s}}{\alpha_s} h^k + o_0\left(h^{p-s}\right) \right),$$

en posant $h = x - a$, et où s est le plus petit indice tel que $\alpha_s \neq 0$.

Proposition 12.12. *$f : I \to \mathbb{K}$ $\mathcal{C}^p$ sur I, $a \in I$. Alors f admet un $DL_p(a)$, donné par la formule de Taylor-Young (proposition 12.8).*

Proposition 12.13. *$f : I \to \mathbb{K}$, $a \in I$. Si f admet un $DL_p(a)$, alors ce DL est unique.*

VI.2 Opérations et développements limités

Proposition 12.14. *$f, g : I \to \mathbb{K}$, $a \in I$. Si f, g ont un $DL_p(a)$ alors $(f+g)$, (fg) et $\frac{1}{f}$ (si $f(a) \neq 0$) ont un $DL_p(a)$.*

VI.3 Intégration de développements limités

Proposition 12.15. *$f : I \to \mathbb{K}$ dérivable sur I, $a \in I$. Si f' a un $DL_p(a)$, alors f a un $DL_{p+1}(a)$. Plus précisément :*

$$f'(x) = \sum_{k=0}^{p} \alpha_k (x-a)^k + o_a\left((x-a)^p\right)$$

$$\implies f(x) = f(a) + \sum_{k=0}^{p} \frac{\alpha_k}{k+1}(x-a)^{k+1} + o_a\left((x-a)^{p+1}\right).$$

Cette propriété reste valable en remplaçant o par $\mathcal{O}$.

VII Utilisation des développements limités

VII.1 Extrema

Proposition 12.16. *$f : I \to \mathbb{R}$ $\mathcal{C}^2$ sur I, $a \in I$. Si $f'(a) = 0$ et $f''(a) \neq 0$, alors f atteint un extremum local en a (qui est un maximum si $f''(a) < 0$, un minimum si $f''(a) > 0$).*

Démonstration. Écrire le $DL_2(a)$ de f et en déduire que $f(x) - f(a) \underset{a}{\sim} \frac{(x-a)^2}{2} f''(a)$. □

VII.2 Position par rapport à la tangente

Proposition 12.17. *$f : I \to \mathbb{R}$. Supposons que f a un $DL_p(a)$ ($p > 1$) du type*

$$f(x) = f(a) + (x-a)f'(a) + (x-a)^p c_p + o_a\left((x-a)^p\right),$$

où $c_p \in \mathbb{R}^*$. On appelle $\mathscr{T}$ la tangente en a à la courbe représentative $\mathscr{C}_f$.

(i) *Si p est impair, $\mathscr{C}_f$ traverse $\mathscr{T}$ localement, i.e. f admet un* point d'inflexion *en a.*

(ii) *Si p est pair, $\mathscr{C}_f$ est soit au-dessus, soit en dessous de $\mathscr{T}$ localement.*

VII.3 Développements asymptotiques

Vocabulaire 12.18 (Développement asymptotique)**.** *Soit f définie dans un voisinage de $\pm\infty$. On dit que f admet un* développement asymptotique *lorsque $x \mapsto f\left(\frac{1}{x}\right)$ admet un $DL_p(0)$.*

Chapitre 13

Arithmétique dans $\mathbb{Z}$

I Définition d'un groupe, d'un anneau et d'un corps

Vocabulaire 13.1 (LCI)**.** *Soit E un ensemble. Une* loi de composition interne *(LCI) sur E est une application $E^2 \to E$.*

Vocabulaire 13.2 (LCE)**.** *Soit E un ensemble. Une* loi de composition externe *(LCE) sur E est une application $\mathbb{K} \times E \to E$.*

Définition 13.3 (Groupe)**.** *Soit G un ensemble, $\diamond$ une LCI sur G. On dit que $(G, \diamond)$ est un* groupe *lorsqu'on a les trois propriétés suivantes :*

(i) Associativité *: $\forall (a,b,c) \in G^3,\ (a \diamond b) \diamond c = a \diamond (b \diamond c)$.*

(ii) Neutre *: $\exists e \in G,\ \forall a \in G,\ e \diamond a = a \diamond e = a$.*

(iii) Inversibilité *: $\forall a \in G,\ \exists a' \in G,\ a \diamond a' = a' \diamond a = e$.*

Si de plus $\diamond$ est commutative, G est dit groupe commutatif.

Définition 13.4 (Anneau)**.** *Soit A un ensemble, $+$ et $\times$ deux LCI sur A. On dit que $(A, +, \times)$ est un* anneau *lorsque :*

(i) *$(A, +)$ est un groupe commutatif de neutre noté 0_A.*

(ii) *$\times$ est associative et distributive par rapport à $+$.*

(iii) *$\times$ admet un neutre noté $1_A \neq 0_A$ dans A.*

Si de plus $\times$ est commutative, A est dit anneau commutatif.

Définition 13.5 (Diviseurs de 0_A)**.** *$(A, +, \times)$ un anneau, $a \in A \backslash \{0_A\}$. a est dit* diviseur de 0_A *lorsque $\exists b \in A \backslash \{0_A\},\ a \times b = 0_A$.*

Définition 13.6 (Anneau intègre)**.** *$(A, +, \times)$ un anneau commutatif. A est dit* intègre *lorsque*

$$\forall (a,b) \in A^2,\ a \times b = 0_A \Longrightarrow a = 0_A \text{ ou } b = 0_A.$$

Autrement dit, A est intègre ssi *0_A n'admet pas de diviseur dans A.*

Définition 13.7 (Corps)**.** *Soit K un ensemble, $+$ et $\times$ deux LCI sur K. On dit que $(K, +, \times)$ est un* corps *lorsque :*

(i) *$(K, +, \times)$ est un anneau commutatif.*

(ii) *Tout élément de $K \backslash \{0_K\}$ admet un inverse pour $\times$ dans K.*

Proposition 13.8. *Si $(K, +, \times)$ est un corps, alors $(K, +, \times)$ est un anneau intègre.*

II Divisibilité dans $\mathbb{Z}$

Définition 13.9 (Divisibilité)**.** $(a,b) \in \mathbb{Z}^2$. *On dit que a divise b, noté $a \mid b$ lorsque* $\exists k \in \mathbb{Z},\ b = ka$.

Remarque 13.10. *Tout élément de $\mathbb{Z}$ divise* 0.

Notation 13.11. $\alpha \in \mathbb{R}$. *On note* $\alpha\mathbb{Z} = \{k\alpha,\ k \in \mathbb{Z}\}$.

Proposition 13.12. $(a,b) \in \mathbb{Z}^2$.

$$a \mid b \iff b\mathbb{Z} \subset a\mathbb{Z}, \tag{i}$$

$$a \mid b \text{ et } b \mid a \iff |a| = |b|. \tag{ii}$$

Corollaire 13.13. $\mid$ *est une relation d'ordre sur* $\mathbb{N}$ *(mais pas sur* $\mathbb{Z}$*).*

Définition 13.14 (Congruences)**.** $n \in \mathbb{N}^*$. $(a,b) \in \mathbb{Z}^2$. *On dit que* $a \equiv b \quad [n]$ *lorsque* $n \mid a - b$.

Proposition 13.15. *La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$, compatible avec $+$ et $\times$:*

$$\forall (a,b,c,d) \in \mathbb{Z}^4,\ \left.\begin{array}{ll} a \equiv b & [n] \\ c \equiv d & [n] \end{array}\right\} \Longrightarrow \left\{\begin{array}{ll} a + c \equiv b + d & [n] \\ a \times c \equiv b \times d & [n] \end{array}\right. .$$

L'ensemble des classes d'équivalence, noté $\mathbb{Z}/n\mathbb{Z}$, possède n éléments distincts.

Notation 13.16. $a \in \mathbb{Z}$. *On note $\overline{a}$ (ou $\overline{a}^n$ lorsqu'il peut y avoir ambiguïté) la classe d'équivalence de a pour la congruence modulo n.*

Définition 13.17. *On définit sur $\mathbb{Z}/n\mathbb{Z}$ les LCI $\overline{+}$ et $\overline{\times}$ par*

$$\overline{a} \overline{+} \overline{b} = \overline{a + b} \quad \text{et} \quad \overline{a} \overline{\times} \overline{b} = \overline{a \times b}.$$

Proposition 13.18. $(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\times})$ *est un anneau commutatif.*

III PGCD et PPCM

III.1 PGCD et PPCM de deux entiers

Définition 13.19 (PGCD)**.** $(a,b) \in \mathbb{Z}^2$. *Si* $a \neq 0$ ou $b \neq 0$, *on appelle* PGCD(a,b), *noté aussi $a \wedge b$, le plus grand entier positif (pour la relation $\leqslant$) divisant a et b. On définit aussi* $0 \wedge 0 = 0$.

Définition 13.20 (PPCM)**.** $(a,b) \in \mathbb{Z}^2$. *Si* $a \neq 0$ et $b \neq 0$, *on appelle* PPCM(a,b), *noté aussi $a \vee b$, le plus petit entier strictement positif (pour la relation $\leqslant$) multiple de a et b. On définit aussi* $0 \vee a = 0$.

Proposition 13.21. $(a,b) \in \mathbb{Z}^2$.

(i) $a \wedge b = |a| \wedge |b|$,

(ii) $0 \wedge a = |a|$,

(iii) $1 \wedge a = 1$,

(iv) $a \vee b = |a| \vee |b|$.

III.2 Algorithme d'Euclide

Lemme 13.22. *$(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. On pose $a = bq + r$, avec $q \in \mathbb{Z}$ et $r \in [\![0, b[\![$. Alors $a \wedge b = b \wedge r$.*

Théorème 13.23 (Algorithme d'Euclide)**.** *$(a,b) \in (\mathbb{N}^*)^2$, $a \geqslant b$. On note $r_0 = a$, $r_1 = b$. Tant que $r_0, \dots, r_{n+1}$ sont tous non nuls, on pose $r_n = r_{n+1}q_{n+1} + r_{n+2}$, avec $q_{n+1} \in \mathbb{Z}$ et $r_{n+2} \in [\![0, r_{n+1}[\![$. Alors il existe $N \in \mathbb{N}$ choisi minimal t.q. $r_{N+1} = 0$, et on a alors $a \wedge b = r_N$.*

Démonstration. Poser $X = \{n \in \mathbb{N},\ \forall k \in [\![0,n]\!],\ r_k > 0\}$. Montrer (par l'absurde) que X est majoré. Comme $X \neq \varnothing$ (car $0 \in X$), choisir alors $N = \max X$ et montrer que $r_{N+1} = 0$ et que $r_N = a \wedge b$. □

Définition 13.24 (Suite de Fibonacci)**.** *On définit la* suite de Fibonacci $(F_n)_{n\in\mathbb{N}}$ *par $F_0 = 0$, $F_1 = 1$ et $\forall n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$.*

Lemme 13.25. *Avec les mêmes notations que dans le théorème 13.23, on a $\forall k \in [\![0, N+1]\!]$, $r_k \geqslant F_{N+1-k}$.*

Démonstration. Par récurrence en utilisant le fait que $\forall k \in [\![0, N-1]\!]$, $r_k \geqslant r_{k+1} + r_{k+2}$ (car $\forall k \in [\![0, N-1]\!]$, $q_{k+1} = \left\lfloor \frac{r_k}{r_{k+1}} \right\rfloor \geqslant 1$). □

Proposition 13.26. *Le nombre d'étapes de l'algorithme d'Euclide est majoré par $\frac{\ln b}{\ln \varphi}$, avec $\varphi = \frac{1+\sqrt{5}}{2}$.*

Démonstration. Montrer d'abord que $\forall p \geqslant 2$, $F_p \geqslant \varphi^{p-2}$, puis en déduire que $\varphi^{N-2} \leqslant F_N \leqslant r_1 = b$, d'où le résultat. □

III.3 Égalité de Bézout

Théorème 13.27 (Égalité de Bézout)**.**

$$\forall (a,b) \in \mathbb{N}^2,\ \exists (u,v) \in \mathbb{Z}^2,\ au + bv = a \wedge b.$$

Démonstration. Se placer dans le cas où $(a,b) \in (\mathbb{N}^*)^2$ et supposer $a > b$. Avec les notations du théorème 13.23, montrer par récurrence que $\forall k \in [\![0, N]\!], \exists (u_k, v_k) \in \mathbb{Z}^2, au_k + bv_k = r_k$. En appliquant ceci avec $k = N$, on obtient le résultat souhaité puisque $r_N = a \wedge b$. □

Proposition 13.28. *$(a,b) \in \mathbb{Z}^2$. L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de $a \wedge b$.*

Corollaire 13.29. *$(a,b) \in \mathbb{N}^2$. $a \wedge b$ est le plus grand entier pour la relation $\mid$ qui divise a et b.*

III.4 PGCD et PPCM de n entiers

Définition 13.30 (PGCD)**.** *$(a_1, \dots, a_n) \in \mathbb{Z}^n$. Si $\exists i \in [\![1,n]\!], a_i \neq 0$, on appelle* $\mathrm{PGCD}(a_1, \dots, a_n)$*, encore noté $a_1 \wedge \cdots \wedge a_n$, le plus grand entier positif (pour la relation $\leqslant$) qui divise chaque a_i, $i \in [\![0,n]\!]$. On définit de plus $0 \wedge \cdots \wedge 0 = 0$.*

Définition 13.31 (PPCM)**.** *$(a_1, \dots, a_n) \in \mathbb{Z}^n$. Si $\forall i \in [\![1,n]\!], a_i \neq 0$, on appelle* $\mathrm{PPCM}(a_1, \dots, a_n)$*, encore noté $a_1 \vee \cdots \vee a_n$, le plus petit entier strictement positif (pour la relation $\leqslant$) qui est multiple de chaque a_i, $i \in [\![0,n]\!]$. On définit de plus $0 \vee a_1 \vee \cdots \vee a_n = 0$.*

Proposition 13.32. $\forall (a,b,c) \in \mathbb{Z}^3,\ a \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge b \wedge c$.

Théorème 13.33 (Égalité de Bézout)**.** $n \geqslant 2$.

$$\forall (a_1,\dots,a_n) \in \mathbb{Z}^n,\ \exists (u_1,\dots,u_n) \in \mathbb{Z}^n,\ \sum_{i=1}^{n} a_i u_i = \bigwedge_{i=1}^{n} a_i.$$

Corollaire 13.34. $(a_1,\dots,a_n) \in \mathbb{Z}^n$. $a_1 \wedge \cdots \wedge a_n$ *est le plus grand entier pour la relation* $\mid$ *qui divise chacun des* a_i, $i \in [\![0,n]\!]$.

IV Nombres premiers entre eux

IV.1 Généralités

Définition 13.35 (Nombres premiers entre eux)**.** $(a,b) \in \mathbb{Z}^2$. *On dit que* a *et* b *sont* premiers entre eux *lorsque* $a \wedge b = 1$.

Théorème 13.36 (Égalité de Bézout)**.** $(a,b) \in (\mathbb{Z}^*)^2$. a *et* b *sont premiers entre eux* ssi $\exists (u,v) \in \mathbb{Z}^2,\ au + bv = 1$.

Corollaire 13.37. $n \in [\![2,+\infty[\![$. $x \in \mathbb{Z}$.

$$\overline{x} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} \iff x \wedge n = 1.$$

Définition 13.38 (Nombres premiers entre eux)**.** $(a_1,\dots,a_n) \in \mathbb{Z}^n$. $a_1,\dots,a_n$ *sont dits* premiers entre eux dans leur ensemble *lorsque* $a_1 \wedge \cdots \wedge a_n = 1$, premiers entre eux deux à deux *lorsque* $\forall (i,j) \in [\![1,n]\!]^2,\ i \neq j \Rightarrow a_i \wedge a_j = 1$.

Proposition 13.39. *Si* $a_1,\dots,a_n$ *sont premiers entre eux deux à deux, alors* $a_1,\dots,a_n$ *sont premiers entre eux dans leur ensemble.*

Lemme 13.40 (Lemme de Gauss)**.** $(a,b,c) \in \mathbb{Z}^3$. *Si* $a \mid bc$ *et* $a \wedge b = 1$, *alors* $a \mid c$.

Démonstration. Écrire l'égalité de Bézout puis multiplier par c. □

Proposition 13.41. $(a,b,c) \in (\mathbb{Z}^*)^3$. $(x_1,\dots,x_n) \in (\mathbb{Z}^*)^n$.

$$a \wedge \left(\prod_{i=1}^{n} x_i\right) = 1 \iff \forall i \in [\![1,n]\!],\ a \wedge x_i = 1. \tag{i}$$

$$a \wedge b = 1 \Longrightarrow \forall (k,\ell) \in (\mathbb{N}^*)^2,\ a^k \wedge b^\ell = 1. \tag{ii}$$

$$\left.\begin{array}{r} b \mid a \\ c \mid a \\ b \wedge c = 1 \end{array}\right\} \Longrightarrow bc \mid a. \tag{iii}$$

$$\forall k \in \mathbb{N}^*,\ k(a \wedge b) = (ka) \wedge (kb). \tag{iv}$$

$$\exists (\alpha,\beta) \in \mathbb{Z}^2,\ \left\{\begin{array}{l} a = (a \wedge b)\alpha \\ b = (a \wedge b)\beta \\ \alpha \wedge \beta = 1 \end{array}\right. . \tag{v}$$

$$\exists ! (c,d) \in \mathbb{Z} \times \mathbb{N}^*,\ \left\{\begin{array}{l} \frac{a}{b} = \frac{c}{d} \\ c \wedge d = 1 \end{array}\right. . \tag{vi}$$

IV.2 PPCM

Proposition 13.42. $(a,b) \in (\mathbb{Z}^*)^2$.

$$a \wedge b = 1 \Longrightarrow a \vee b = |ab|. \tag{i}$$

$$(a \wedge b)(a \vee b) = |ab|. \tag{ii}$$

Corollaire 13.43. $(a,b) \in (\mathbb{Z}^*)^2$. *L'ensemble des multiples communs à a et b est égal à l'ensemble des multiples de $a \vee b$.*

Corollaire 13.44. $(a,b) \in \mathbb{N}^2$. *$a \vee b$ est le plus petit entier pour la relation $\mid$ qui est multiple de a et b.*

Proposition 13.45. $\forall (a,b,c) \in (\mathbb{Z}^*)^3$, $a \vee (b \vee c) = (a \vee b) \vee c = a \vee b \vee c$.

Proposition 13.46. $\forall (a,b) \in (\mathbb{Z}^*)^2$, $\forall k \in \mathbb{N}^*$, $k(a \vee b) = (ka) \vee (kb)$.

V Nombres premiers

V.1 Généralités

Définition 13.47. $p \in [\![2, +\infty[\![$. *p est dit* premier *lorsque p n'admet comme diviseurs positifs que 1 et lui-même.*

Notation 13.48. *On note $\mathbb{P}$ l'ensemble des nombres premiers et, pour $n \in \mathbb{Z}$, $\mathbb{P}_n = \{p \in \mathbb{P},\ p \mid n\}$.*

Proposition 13.49.

$$\forall p \in \mathbb{P},\ \forall a \in \mathbb{Z},\ a \wedge p = 1 \text{ ou } p \mid a. \tag{i}$$

$$\forall (p,q) \in \mathbb{P}^2,\ p \neq q \Longrightarrow p \wedge q = 1. \tag{ii}$$

$$\forall p \in \mathbb{P},\ \forall (x_1, \ldots, x_n) \in \mathbb{Z}^n,\ p \mid \left(\prod_{i=1}^{n} x_i \right) \Longleftrightarrow \exists i \in [\![1,n]\!],\ p \mid x_i. \tag{iii}$$

Lemme 13.50. $\forall p \in \mathbb{P},\ \forall k \in [\![1, p-1]\!],\ p \mid \binom{p}{k}$.

Théorème 13.51 (Petit théorème de Fermat)**.** $\forall p \in \mathbb{P},\ \forall n \in \mathbb{N},\ n^p \equiv n \quad [p]$.

Démonstration. Par récurrence à l'aide du binôme de Newton (théorème 1.16) et du lemme 13.50. □

V.2 Théorème fondamental de l'arithmétique

Proposition 13.52. *Tout entier supérieur ou égal à 2 admet un diviseur premier.*

Proposition 13.53. *$\mathbb{P}$ est infini.*

Démonstration. Par l'absurde : supposer $\mathbb{P} = \{p_1, \cdots, p_N\}$ et considérer l'entier $A = 1 + \prod_{i=1}^{N} p_i$. □

Définition 13.54 (Valuation p-adique)**.** $p \in \mathbb{P}$, $n \in \mathbb{N}$. *On appelle* valuation p-adique de n *l'entier*

$$v_p(n) = \max\{k \in \mathbb{N},\ p^k \mid n\}.$$

Théorème 13.55 (Théorème fondamental de l'arithmétique)**.**

$$\forall n \in [\![2, +\infty[\![,\ \exists (p_1, \dots, p_k) \in \mathbb{P}^k,\ \exists (\alpha_1, \dots, \alpha_k) \in (\mathbb{N}^*)^k,\ n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

De plus, cette écriture est unique à l'ordre près des facteurs (en supposant $\forall (i,j) \in [\![1, r]\!]^2,\ i \neq j \Longrightarrow p_i \neq p_j$*).*

Démonstration. Existence. Par récurrence forte. Unicité. Supposer $n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{\ell} q_i^{\beta_i}$. Montrer que $\forall i \in [\![1, k]\!],\ \exists j \in [\![1, \ell]\!],\ p_i = q_j$, et inversement. En déduire que $\{p_1, \dots, p_k\} = \{q_1, \dots, q_\ell\}$. Montrer ensuite que $\forall i \in [\![1, k]\!],\ \alpha_i = v_{p_i}(n)$ et $\forall j \in [\![1, \ell]\!],\ \beta_i = v_{q_i}(n)$. D'où l'unicité de l'écriture. □

Remarque 13.56. $n \in \mathbb{N}^*$*.Le théorème précédent peut s'écrire*

$$n = \prod_{p \in \mathbb{P}_n} p^{v_p(n)} = \prod_{p \in \mathbb{P}} p^{v_p(n)}.$$

V.3 Conséquences

Proposition 13.57. $(a, b) \in (\mathbb{N}^*)^2$.

$$\forall p \in \mathbb{P},\ p \mid a \Longleftrightarrow v_p(a) > 0. \tag{i}$$

$$\forall p \in \mathbb{P},\ v_p(ab) = v_p(a) + v_p(b). \tag{ii}$$

$$a \mid b \Longleftrightarrow \forall p \in \mathbb{P},\ v_p(a) \leqslant v_p(b). \tag{iii}$$

Corollaire 13.58. $(a, b) \in (\mathbb{N}^*)^2$.

$$a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))}, \tag{i}$$

$$a \vee b = \prod_{p \in \mathbb{P}} p^{\max(v_p(a), v_p(b))}. \tag{ii}$$

VI Calculs dans $\mathbb{Z}/n\mathbb{Z}$

VI.1 Corps

Proposition 13.59. $n \in [\![2, +\infty[\![$. $\mathbb{Z}/n\mathbb{Z}$ *est un corps* ssi $n \in \mathbb{P}$.

VI.2 Résolution d'équations dans $\mathbb{Z}/n\mathbb{Z}$

Méthode 13.60. $(a, b, n) \in (\mathbb{Z}^*)^3$*. On considère l'équation*

$$ax \equiv b \quad [n]\,.$$

On note $d = a \wedge n$.

(i) *Si* $d \nmid b$*, alors il n'y a aucune solution.*

(ii) *Si* $d \mid b$*, poser* $a = da'$, $n = dn'$ *et* $b = db'$ *tels que* $a' \wedge n' = 1$*. On a alors* $ax \equiv b \quad [n] \Longleftrightarrow a'x \equiv b' \quad [n']$*. Utiliser alors l'inversibilité de* $\overline{a'}$ *dans* $\mathbb{Z}/n'\mathbb{Z}$ *pour résoudre l'équation.*

VI.3 Systèmes d'équations dans $\mathbb{Z}/n\mathbb{Z}$

Méthode 13.61. *$(a,b,m,n) \in (\mathbb{Z}^*)^4$, $m \wedge n = 1$. On considère le système*

$$\begin{cases} x \equiv a \quad [m] \\ x \equiv b \quad [n] \end{cases}.$$

Pour le résoudre, on recherche d'abord une solution particulière. On sait (théorème 13.27) que $\exists (u,v) \in \mathbb{Z}^2$, $mu + nv = 1$. Alors $x_0 = mub + nva$ convient. On a ainsi

$$\begin{cases} x \equiv a \quad [m] \\ x \equiv b \quad [n] \end{cases} \iff \begin{cases} x \equiv x_0 \quad [m] \\ x \equiv x_0 \quad [n] \end{cases} \iff x \equiv x_0 \quad [mn]\,.$$

Corollaire 13.62. *On a construit une bijection*

$$\varphi : \left| \begin{array}{c} (\mathbb{Z}/mn\mathbb{Z}) \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ \overline{x}^{mn} \longmapsto (\overline{x}^m, \overline{x}^n) \end{array} \right. .$$

VII Indicatrice d'Euler

Définition 13.63 (Indicatrice d'Euler)**.** *$n \in [\![2, +\infty[\![$. On appelle* indicatrice d'Euler *de n, notée $\varphi(n)$, le nombre de nombres premiers avec n compris entre 1 et n.*

Proposition 13.64.

$$\forall p \in \mathbb{P},\ \varphi(p) = p - 1. \tag{i}$$

$$\forall p \in \mathbb{P},\ \forall k \in \mathbb{N}^*,\ \varphi\left(p^k\right) = p^k - p^{k-1}. \tag{ii}$$

$$\forall n \in [\![2, +\infty[\![,\ n = \sum_{d|n} \varphi(d). \tag{iii}$$

Chapitre 14

Groupes, Anneaux et Corps

I Groupes

I.1 Définitions et généralités

Définition 14.1 (Groupe)**.** *Soit G un ensemble, $\diamond$ une LCI sur G. On dit que $(G, \diamond)$ est un* groupe *lorsqu'on a les trois propriétés suivantes :*

(i) Associativité *: $\forall (a,b,c) \in G^3,\ (a \diamond b) \diamond c = a \diamond (b \diamond c)$.*

(ii) Neutre *: $\exists e \in G,\ \forall a \in G,\ e \diamond a = a \diamond e = a$.*

(iii) Inversibilité *: $\forall a \in G,\ \exists a' \in G,\ a \diamond a' = a' \diamond a = e$.*

Si de plus $\diamond$ est commutative, G est dit groupe commutatif.

Proposition 14.2. *Soit $(G, \diamond)$ un groupe. Alors le neutre est unique, et tout élément de G a un unique inverse.*

Notation 14.3. *On utilise principalement deux notations :*

(i) Notation additive. *Soit $(G, +)$ un groupe. On note 0_G son neutre ; pour $x \in G$, $(-x)$ est l'opposé de x. Pour $n \in \mathbb{Z}_+^*$, $nx = x + \cdots + x$ (n fois), $0x = 0_G$, et pour $n \in \mathbb{Z}_-^*$, $nx = (-n)(-x)$.*

(ii) Notation multiplicative. *Soit $(G, \times)$ un groupe. On note 1_G son neutre ; pour $x \in G$, x^{-1} est l'inverse de x. Pour $n \in \mathbb{Z}_+^*$, $x^n = x \times \cdots \times x$ (n fois), $x^0 = 1_G$, et pour $n \in \mathbb{Z}_-^*$, $x^n = \left(x^{-1}\right)^{-n}$.*

Proposition 14.4. *$(G, \diamond)$ un groupe. $\forall (x,y) \in G^2,\ (x \diamond y)^{-1} = y^{-1} \diamond x^{-1}$.*

Exemple 14.5. *$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathbb{R}^{\mathbb{R}}, +)$, $(\mathbb{R}^{\mathbb{N}}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}_n, \times)$ sont des groupes commutatifs.*

Notation 14.6. *Pour $X \neq \varnothing$, on note $\mathfrak{S}_X$ l'ensemble des bijections $X \to X$ (dites aussi permutations).*

Exemple 14.7. *$(\mathfrak{S}_X, \circ)$ est un groupe en général non commutatif.*

Définition 14.8 (Produit cartésien de groupes)**.** *$(G, \diamond)$ et $(H, \circ)$ deux groupes. On définit la LCI $\star$ sur $G \times H$ par*

$$\star : \left| \begin{array}{c} (G \times H) \times (G \times H) \longrightarrow G \times H \\ ((x,x'),(y,y')) \longmapsto (x \diamond y, x' \circ y') \end{array} \right. .$$

Alors $(G \times H, \star)$ est un groupe, dit produit cartésien *de G et H.*

I.2 Sous-groupes

Définition 14.9 (Sous-groupe)**.** *$(G, \diamond)$ un groupe. $H \subset G$, $H \neq \varnothing$. H est dit* sous-groupe *de G (pour $\diamond$) lorsqu'on a les deux propriétés suivantes :*

(i) *H est* stable *par $\diamond$ (i.e. $\forall (x, y) \in H^2$, $(x \diamond y) \in H$).*

(ii) *$(H, \diamond)$ est un groupe.*

Proposition 14.10. *$(G, \diamond)$ un groupe. $H \subset G$, $H \neq \varnothing$. H est un sous-groupe de G* ssi *on a les trois propriétés suivantes :*

(i) *H est stable par $\diamond$.*

(ii) *Le neutre de G appartient à H.*

(iii) *$\forall x \in H$, $x^{-1} \in H$.*

Proposition 14.11. *Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$. De plus, n ainsi déterminé est unique.*

Démonstration. Vérifier d'abord que les $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. Prendre alors H un sous-groupe de $\mathbb{Z}$. Supposer $H \neq \{0\}$ (dans le cas contraire $H = 0\mathbb{Z}$) et choisir $n = \min H \cap \mathbb{N}^*$. L'inclusion $n\mathbb{Z} \subset H$ est claire. Prendre alors $h \in H$ et utiliser la division euclidienne de h par n pour montrer que $h \in n\mathbb{Z}$, i.e. $H \subset n\mathbb{Z}$. Montrer ensuite l'unicité de n. □

Définition 14.12 (Centre)**.** *$(G, \diamond)$ un groupe. On appelle* centre *de G l'ensemble*

$$Z(G) = \{x \in G,\ \forall y \in G,\ x \diamond y = y \diamond x\}.$$

Proposition 14.13. *$(G, \diamond)$ un groupe. Alors $Z(G)$ est un sous-groupe de G.*

Proposition 14.14. *$(G, \diamond)$ un groupe. $(H_i)_{i \in I}$ une famille de sous-groupes de G, où I est un ensemble quelconque. Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.*

Théorème 14.15 (Théorème de Lagrange)**.** *$(G, \diamond)$ un groupe fini. H un sous-groupe de G. Alors le cardinal de H divise le cardinal de G.*

Démonstration. Introduire sur G la relation $\mathcal{R}$ définie par $x \mathcal{R} y$ ssi $xH = yH$. Montrer que $\mathcal{R}$ est une relation d'équivalence. Montrer alors que $\forall x \in G$, $\mathrm{Cl}(x) = xH$. Remarquer que xH et H sont en bijection, donc ont le même cardinal. En utilisant le fait que $(\mathrm{Cl}(x))_{x \in G}$ est une partition de G, obtenir le résultat. □

I.3 Groupes engendrés par une partie

Définition 14.16 (Groupe engendré par une partie)**.** *$(G, \diamond)$ un groupe. $A \subset G$. On appelle* groupe engendré par *A, noté $\langle A \rangle$, le plus petit sous-groupe de G contenant A.*

Proposition 14.17. *$(G, \diamond)$ un groupe. $A \subset G$. On note X l'ensemble des sous-groupes de G contenant A. Si $A \neq \varnothing$, alors $\langle A \rangle = \bigcap_{H \in X} H$. Si $A = \varnothing$, $\langle A \rangle = \{e_G\}$, où e_G désigne le neutre de G.*

Proposition 14.18. *$(G, \diamond)$ un groupe. $g \in G$. Alors $\langle g \rangle = \{g^n,\ n \in \mathbb{Z}\}$.*

Vocabulaire 14.19 (Groupe monogène)**.** *$(G, \diamond)$ un groupe. On dit que G est* monogène *lorsque $\exists g \in G, G = \langle g \rangle$. g est alors dit* générateur *de G. On dit de plus que G est* cyclique *si G est monogène fini.*

Proposition 14.20. *$(G, \diamond)$ un groupe fini de cardinal n et de neutre e_G. $g \in G \backslash \{e_G\}$. On note $q = \min\{r \in \mathbb{N}^*,\ g^r = e_G\}$. Alors :*

(i) $g^n = e_G$,

(ii) $\langle g \rangle = \{g^k,\ k \in [\![0, q-1]\!]\}$,

(iii) $\text{card}(\langle g \rangle) = q$.

I.4 Morphismes de groupes

Définition 14.21 (Morphisme de groupes)**.** *$(G, \diamond)$ et $(H, \circ)$ deux groupes. On dit que $\phi : G \to H$ est un* morphisme de groupes *lorsque*

$$\forall (x, y) \in G^2,\ \phi(x \diamond y) = \phi(x) \circ \phi(y).$$

Proposition 14.22. *$(G, \diamond)$ et $(H, \circ)$ deux groupes de neutres respectifs e_G et e_H. $\phi : G \to H$ un morphisme de groupes.*

$$\phi(e_G) = e_H \qquad et \qquad \forall x \in G,\ \phi\left(x^{-1}\right) = (\phi(x))^{-1}.$$

Proposition 14.23. *$(G, \diamond)$ et $(H, \circ)$ deux groupes. $\phi : G \to H$ un morphisme de groupes. G' et H' des sous-groupes de G et H respectivement. Alors $\phi(G')$ est un sous-groupe de H et $\phi^{-1}(H')$ est un sous-groupe de G.*

Définition 14.24 (Noyau)**.** *$(G, \diamond)$ et $(H, \circ)$ deux groupes de neutres respectifs e_G et e_H. $\phi : G \to H$ un morphisme de groupes. On définit*

$$\text{Ker}\,\phi = \phi^{-1}(\{e_H\}).$$

D'après la proposition 14.23, $\text{Ker}\,\phi$ *est un sous-groupe de G.*

Proposition 14.25. *$(G, \diamond)$ et $(H, \circ)$ deux groupes de neutres respectifs e_G et e_H. $\phi : G \to H$ un morphisme de groupes.*

$$\text{Ker}\,\phi = \{e_G\} \iff \phi \text{ est injective.}$$

Vocabulaire 14.26. *$(G, \diamond)$ et $(H, \circ)$ deux groupes. $\phi : G \to H$ un morphisme de groupes.*

(i) *ϕ est dit* isomorphisme *si ϕ est bijectif.*

(ii) *ϕ est dit* endomorphisme *si $G = H$.*

(iii) *ϕ est dit* automorphisme *si ϕ est un endomorphisme bijectif.*

Vocabulaire 14.27. *$(G, \diamond)$ et $(H, \circ)$ deux groupes. On dit que G et H sont* isomorphes*, et on note $G \simeq H$, lorsqu'il existe un isomorphisme $G \to H$.*

Proposition 14.28. *$(G, \diamond)$ un groupe cyclique de cardinal n. Alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 14.29. *$(G, \diamond)$ un groupe monogène infini. Alors G est isomorphe à $\mathbb{Z}$.*

II Anneaux et corps

II.1 Généralités

Définition 14.30 (Anneau)**.** *Soit A un ensemble, $+$ et $\times$ deux LCI sur A. On dit que $(A,+,\times)$ est un* anneau *lorsque :*

(i) *$(A,+)$ est un groupe commutatif de neutre noté 0_A.*

(ii) *$\times$ est associative et distributive par rapport à $+$.*

(iii) *$\times$ admet un neutre noté $1_A \neq 0_A$ dans A.*

Si de plus $\times$ est commutative, A est dit anneau commutatif.

Définition 14.31 (Diviseurs de 0_A)**.** *$(A,+,\times)$ un anneau, $a \in A\backslash\{0_A\}$. a est dit* diviseur de 0_A *lorsque $\exists b \in A\backslash\{0_A\}$, $a \times b = 0_A$.*

Définition 14.32 (Anneau intègre)**.** *$(A,+,\times)$ un anneau commutatif. A est dit* intègre *lorsque*

$$\forall (a,b) \in A^2,\ a \times b = 0_A \Longrightarrow a = 0_A \text{ ou } b = 0_A.$$

Autrement dit, A est intègre ssi *0_A n'admet pas de diviseur dans A.*

Définition 14.33 (Corps)**.** *Soit K un ensemble, $+$ et $\times$ deux LCI sur K. On dit que $(K,+,\times)$ est un* corps *lorsque :*

(i) *$(K,+,\times)$ est un anneau commutatif.*

(ii) *Tout élément de $K\backslash\{0_K\}$ admet un inverse pour $\times$ dans K.*

Proposition 14.34. *Si $(K,+,\times)$ est un corps, alors $(K,+,\times)$ est un anneau intègre.*

Exemple 14.35. *$(\mathbb{M}_2(\mathbb{R}),+,\times)$, $(\mathbb{Z}/n\mathbb{Z},+,\times)$, $(\mathcal{P}(E),\triangle,\cap)$ sont des anneaux en général non intègres.*

Exemple 14.36. *$(\mathbb{C},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{Q},+,\times)$ sont des corps.*

Définition 14.37 (Sous-anneau)**.** *$(A,+,\times)$ anneau, $B \subset A$. B est dit* sous-anneau *de A lorsque $(B,+,\times)$ est un anneau.*

Proposition 14.38. *$(A,+,\times)$ anneau, $B \subset A$. B est un sous-anneau de A* ssi *les trois propriétés suivantes sont vérifiées :*

(i) *$(B,+)$ est un sous-groupe de $(A,+)$.*

(ii) *$\times$ est stable dans B.*

(iii) *$1_A \in B$.*

Définition 14.39 (Sous-corps)**.** *$(K,+,\times)$ corps, $B \subset A$. B est dit* sous-corps *de A lorsque $(B,+,\times)$ est un corps.*

Proposition 14.40. *$(K,+,\times)$ corps, $B \subset A$. B est un sous-corps de A* ssi *les quatre propriétés suivantes sont vérifiées :*

(i) *$(B,+)$ est un sous-groupe de $(A,+)$.*

(ii) *$\times$ est stable dans B.*

(iii) *$1_A \in B$.*

(iv) *$\forall x \in B\backslash\{0_A\}$, $x^{-1} \in B$.*

Exemple 14.41. *$\mathbb{Z}[i] = \{a+bi,\ (a,b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.*

Notation 14.42. *$(A,+,\times)$ anneau. On note A^* (ou A' ou $U(A)$) l'ensemble des éléments inversibles de A (pour $\times$).*

Proposition 14.43. *$(A,+,\times)$ anneau. $(A^*,\times)$ est un groupe.*

II.2 Règles de calcul

Définition 14.44. *$(A,+,\times)$ anneau. $(a,b)\in A^2$ t.q. $ab=ba$ et $n\in\mathbb{N}^*$.*

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

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

II.3 Morphismes d'anneaux et de corps

Définition 14.45 (Morphisme d'anneaux ou de corps)**.** *$(A,+,\times)$ et $(B,+,\times)$ deux anneaux (ou corps). On dit que $\phi:A\to B$ est un* morphisme d'anneaux *(ou de corps) lorsque :*

$$\forall(a,b)\in A^2,\ \phi(a+b)=\phi(a)+\phi(b), \tag{i}$$

$$\forall(a,b)\in A^2,\ \phi(ab)=\phi(a)\phi(b), \tag{ii}$$

$$\phi(1_A)=1_B. \tag{iii}$$

Vocabulaire 14.46. *$(A,+,\times)$ et $(B,+,\times)$ deux anneaux (ou corps). $\phi:A\to B$ un morphisme d'anneaux (ou de corps).*

(i) *ϕ est dit* isomorphisme *si ϕ est bijectif.*

(ii) *ϕ est dit* automorphisme *si ϕ est un isomorphisme et $A=B$.*

Proposition 14.47. *id est le seul automorphisme de $(\mathbb{Z},+,\times)$, de $(\mathbb{Q},+,\times)$ et de $(\mathbb{R},+,\times)$.*

Démonstration. Soit ψ un automorphisme de $(\mathbb{R},+,\times)$ (ou de $(\mathbb{Z},+,\times)$ ou de $(\mathbb{Q},+,\times)$). Dans tous les cas, commencer par montrer que $\forall n\in\mathbb{Z},\ \psi(n)=n$. Montrer ensuite que $\forall r\in\mathbb{Q},\ \psi(r)=r$. Montrer que $\psi\nearrow$. Pour $x\in\mathbb{R}$ construire deux suites $(u_n)\in\mathbb{Q}^{\mathbb{N}}$ et $(v_n)\in\mathbb{Q}^{\mathbb{N}}$ t.q. $\forall n\in\mathbb{N},\ u_n\leqslant x\leqslant v_n$ et $\lim_{n\to+\infty}u_n=\lim_{n\to+\infty}v_n=x$. En déduire que $\psi(x)=x$. □

Proposition 14.48. *$(A,+,\times)$ et $(B,+,\times)$ deux anneaux. $\phi:A\to B$ un isomorphisme d'anneaux. Alors $\phi(A^*)=B^*$.*

Proposition 14.49. *$(A,+,\times)$ et $(B,+,\times)$ deux anneaux. $A\times B$ est un anneau muni des lois produits, et $(A\times B)^*=A^*\times B^*$.*

Lemme 14.50 (Lemme chinois)**.** *$(m,n)\in(\mathbb{N}^*)^2$, $m\wedge n=1$. Alors l'application*

$$\varphi:\left|\begin{array}{c}(\mathbb{Z}/mn\mathbb{Z})\longrightarrow(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})\\ \overline{x}^{mn}\longmapsto(\overline{x}^m,\overline{x}^n)\end{array}\right.$$

est un isomorphisme d'anneaux.

Corollaire 14.51. *$(m,n)\in[\![2,+\infty[\![^2$, $m\wedge n=1$. En notant φ l'indicatrice d'Euler (voir définition 13.63), on a :*

$$\varphi(mn)=\varphi(m)\varphi(n).$$

Corollaire 14.52. *$n\in[\![2,+\infty[\![$. Alors*

$$\varphi(n)=\prod_{p\in\mathbb{P}_n}\varphi\left(p^{v_p(n)}\right)=\prod_{p\in\mathbb{P}_n}p^{v_p(n)}\left(1-\frac{1}{p}\right)=n\prod_{p\in\mathbb{P}_n}\left(1-\frac{1}{p}\right).$$

Théorème 14.53 (Théorème d'Euler)**.** *$(a,n)\in(\mathbb{N}^*)^2$, $a\wedge n=1$.*

$$a^{\varphi(n)}\equiv 1\quad[n].$$

II.4 Idéaux d'un anneau

Notation 14.54. *Dans ce paragraphe,* $(A, +, \times)$ *est un anneau commutatif.*

Définition 14.55 (Idéal)**.** $I \subset A$. *I est dit* idéal *de A lorsque :*

(i) $(I, +)$ *est un sous-groupe additif de* $(A, +)$.

(ii) $\forall a \in A,\ aI \subset I$.

Proposition 14.56. *Les idéaux de* $\mathbb{Z}$ *sont les* $n\mathbb{Z}$, $n \in \mathbb{N}$.

Proposition 14.57. I, J *deux idéaux de A. Alors* $I \cap J$ *et* $I + J = \{x + y,\ (x, y) \in I \times J\}$ *sont des idéaux de A.*

Proposition 14.58. $\alpha \in A$. *Alors* $\alpha A = \{\alpha x,\ x \in A\}$ *est un idéal de A.*

Définition 14.59 (Idéal principal)**.** *On dit qu'un idéal I de A est* principal *si* $\exists \alpha \in A, I = \alpha A$. *On dit qu'un anneau est* principal *si tous ses idéaux sont principaux.*

Proposition 14.60. $(m, n) \in (\mathbb{N}^*)^2$.

$$m\mathbb{Z} + n\mathbb{Z} = (m \wedge n)\mathbb{Z} \qquad et \qquad m\mathbb{Z} \cap n\mathbb{Z} = (m \vee n)\mathbb{Z}.$$

Remarque 14.61. *On démontre cette propriété en utilisant uniquement les définitions 13.19 et 13.20, et aucune autre propriété du* PGCD *et du* PPCM. *De plus, on peut ainsi définir le* PGCD *et le* PPCM *dans des anneaux principaux autres que* $\mathbb{Z}$.

Chapitre 15

Polynômes

I Généralités

I.1 Définition

Définition 15.1 (Suite à support fini)**.** *On dit qu'une suite $u \in \mathbb{K}^{\mathbb{N}}$ est* à support fini *si l'ensemble $\{n \in \mathbb{N},\ u_n \neq 0\}$, dit* support *de u, est fini.*

Notation 15.2. *Dans la section I, on notera $\mathcal{A}$ l'ensemble des suites à support fini.*

I.2 Lois de composition interne

Définition 15.3 (LCI sur $\mathcal{A}$)**.** *On définit les LCI $+$ et $\times$, pour $(u, v) \in \mathcal{A}^2$, par :*

$$u + v = (u_n + v_n)_{n\in\mathbb{N}} \qquad et \qquad u \times v = \left(\sum_{i=0}^{n} u_i v_{n-i}\right)_{n\in\mathbb{N}}.$$

Proposition 15.4. *$(\mathcal{A}, +, \times)$ est un anneau commutatif.*

Notation 15.5. *On définit, pour $n \in \mathbb{N}$, la suite $e_n \in \mathcal{A}$ par*

$$\forall k \in \mathbb{N},\ (e_n)_k = \begin{cases} 1 & si\ k = n \\ 0 & sinon \end{cases}.$$

Proposition 15.6. $\forall n \in \mathbb{N},\ (e_1)^n = e_n$.

I.3 Loi de composition externe

Définition 15.7 (LCE sur $\mathcal{A}$)**.** *On définit la LCE $\cdot$, pour $(\lambda, u) \in \mathbb{K} \times \mathcal{A}$, par :*

$$\lambda \cdot u = (\lambda u_n)_{n\in\mathbb{N}}.$$

Vocabulaire 15.8 (Combinaison linéaire)**.** *Soit $(u_i)_{i\in\mathbb{N}}$ une famille d'éléments de $\mathcal{A}$. On appelle* combinaison linéaire *(finie) de $(u_i)_{i\in\mathbb{N}}$ toute suite du type $\sum_{k=0}^{p} \lambda_{i_k} u_{i_k}$, où $(\lambda_{i_0}, \ldots, \lambda_{i_p}) \in \mathbb{K}^{p+1}$.*

Proposition 15.9. *Toute suite $u \in \mathcal{A}$ est combinaison linéaire finie de la famille $(e_n)_{n\in\mathbb{N}}$. De plus u s'écrit $u = \sum_{k\in\mathbb{N}} u_k e_k$, et cette écriture est unique.*

Notation 15.10. *On note $X = e_1$, et $\forall n \in \mathbb{N}$, $X^n = (e_1)^n = e_n$. Soit $P \in \mathcal{A}$. On a donc montré que P s'écrit de manière unique*

$$P = \sum_{k\in\mathbb{N}} \lambda_k X^k,$$

où $\lambda = P \in \mathcal{A}$. L'ensemble $\mathcal{A}$ est noté $\mathbb{K}[X]$, ses éléments sont dits polynômes, *et les $(\lambda_k)_{k\in\mathbb{N}}$ sont dits* coefficients *de P.*

Vocabulaire 15.11. *Pour $k \in \mathbb{N}$, $\lambda_k \in \mathbb{K}$, le polynôme $\lambda_k X^k$ est dit* monôme. *De plus, tout polynôme de la forme $\lambda_0 X^0$ est dit* constant.

I.4 Composition de deux polynômes

Définition 15.12 (Composition)**.** *$(P, Q) \in \mathbb{K}[X]^2$, avec $P = \sum_{k\in\mathbb{N}} \lambda_k X^k$. On définit alors*

$$P \circ Q = \sum_{k\in\mathbb{N}} \lambda_k Q^k \in \mathbb{K}[X].$$

Proposition 15.13.

$$\forall (P, Q, R) \in \mathbb{K}[X]^3,\ (P + Q) \circ R = (P \circ R) + (Q \circ R), \tag{i}$$

$$\forall (P, Q, R) \in \mathbb{K}[X]^3,\ (P \times Q) \circ R = (P \circ R) \times (Q \circ R), \tag{ii}$$

$$\forall (P, Q, R) \in \mathbb{K}[X]^3,\ (P \circ Q) \circ R = P \circ (Q \circ R). \tag{iii}$$

Définition 15.14 (Parité)**.** *$P \in \mathbb{K}[X]$. On dit que P est* pair *lorsque $P \circ (-X) = P$; on dit que P est* impair *lorsque $P \circ (-X) = -P$.*

Proposition 15.15. *$P \in \mathbb{K}[X]$, avec $P = \sum_{k\in\mathbb{N}} \lambda_k X^k$.*

$$P \text{ est pair} \iff \forall k \in \mathbb{N},\ \lambda_{2k+1} = 0 \iff \exists Q \in \mathbb{K}[X],\ P = Q \circ X^2. \tag{i}$$

$$P \text{ est impair} \iff \forall k \in \mathbb{N},\ \lambda_{2k} = 0 \iff \exists Q \in \mathbb{K}[X],\ P = X\left(Q \circ X^2\right). \tag{ii}$$

Notation 15.16. *$(P, Q) \in \mathbb{K}[X]^2$. On notera souvent $P(Q)$ à la place de $P \circ Q$.*

II Degré d'un polynôme

II.1 Généralités

Définition 15.17 (Degré)**.** *$A = \sum_{k\in\mathbb{N}} a_k X^k \in \mathbb{K}[X]$. Si $A \neq 0$, l'ensemble $\{k \in \mathbb{N},\ a_k \neq 0\}$ admet un plus grand élément noté $\deg A$, et dit* degré *de A. Si $A = 0$, alors $\deg A = -\infty$.*

Proposition 15.18. *$(A, B) \in \mathbb{K}[X]^2$.*

(i) $\deg A \in \mathbb{N} \iff A \neq 0$,

(ii) $\deg A \in \mathbb{N}^*$ ssi *A non constant,*

(iii) $\deg(A + B) \leqslant \max(\deg A, \deg B)$ *avec égalité dès que* $\deg A \neq \deg B$,

(iv) $\deg(AB) = \deg A + \deg B$.

Corollaire 15.19. $(A_1, \dots, A_p) \in \mathbb{K}[X]^p$.

$$\deg\left(\sum_{i=1}^{p} A_i\right) \leqslant \max_{i\in[\![1,p]\!]} (\deg A_i)\,, \tag{i}$$

$$\deg\left(\prod_{i=1}^{p} A_i\right) = \sum_{i=1}^{p} \deg A_i. \tag{ii}$$

Vocabulaire 15.20. $A = \sum_{k\in\mathbb{N}} a_k X^k \in \mathbb{K}[X]$. *Le coefficient* a_0 *est dit* coefficient constant. *Si* $A \neq 0$, *le coefficient* $a_{\deg A}$ *est dit* coefficient dominant, *et le monôme* $a_{\deg A} X^{\deg A}$ *est dit* monôme de plus haut degré.

Notation 15.21. $m \in \mathbb{N}$. *On note* $\mathbb{K}_m[X] = \{P \in \mathbb{K}[X],\ \deg P \leqslant m\}$.

Proposition 15.22. $A \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$. *Alors* $\deg(\lambda A) = \begin{cases} \deg A \text{ si } \lambda \neq 0 \\ -\infty \text{ sinon} \end{cases}$.

Proposition 15.23. $m \in \mathbb{N}$. $\mathbb{K}_m[X]$ *est stable par combinaison linéaire.*

II.2 Intégrité de $\mathbb{K}[X]$ et éléments inversibles

Proposition 15.24. $(\mathbb{K}[X], +, \times)$ *est un anneau intègre.*

Corollaire 15.25. $(A, B, C) \in \mathbb{K}[X]\backslash\{0\} \times \mathbb{K}[X]^2$.

$$AB = AC \Longrightarrow B = C.$$

Proposition 15.26. $\mathbb{K}[X]^* = \{P \in \mathbb{K}[X],\ \deg P = 0\}$. *Autrement dit, les éléments inversibles de* $\mathbb{K}[X]$ *sont les polynômes constants non nuls.*

II.3 Degré et composition

Proposition 15.27. $(A, B) \in \mathbb{K}[X]^2$, B *non constant. Alors* $\deg(A \circ B) = \deg A \deg B$.

III Divisibilité dans $\mathbb{K}[X]$

Définition 15.28 (Divisibilité)**.** $(A, B) \in \mathbb{K}[X]^2$. *On dit que* A divise B, *noté* $A \mid B$ *lorsque* $\exists C \in \mathbb{K}[X],\ B = AC$.

Notation 15.29. $A \in \mathbb{K}[X]$. *On note* $A\mathbb{K}[X] = \{AC,\ C \in \mathbb{K}[X]\}$.

Proposition 15.30. $A \in \mathbb{K}[X]$. $A\mathbb{K}[X]$ *est un idéal de* $\mathbb{K}[X]$.

Définition 15.31 (Polynômes associés)**.** $(A, B) \in \mathbb{K}[X]^2$. A *et* B *sont dits* associés *lorsque* $A \mid B$ *et* $B \mid A$.

Proposition 15.32. $(A, B) \in \mathbb{K}[X]^2$. A *et* B *sont associés* ssi $\exists \lambda \in \mathbb{K}^*,\ B = \lambda A$.

Vocabulaire 15.33. $A = \sum_{k\in\mathbb{N}} a_k X^k \in \mathbb{K}[X]\backslash\{0\}$. A *est dit* unitaire *(ou* normalisé*) lorsque* $a_{\deg A} = 1$. *Le polynôme* $A^* = \frac{1}{a_{\deg A}} A$ *est dit* polynôme normalisé *de* A.

Proposition 15.34. *Deux polynômes unitaires associés sont égaux.*

Proposition 15.35. $A \in \mathbb{K}[X]\backslash\{0\}$. *Alors* A^* *est l'unique polynôme unitaire de* $\mathbb{K}[X]$ *vérifiant* $A^*\mathbb{K}[X] = A\mathbb{K}[X]$.

Proposition 15.36.

$$\forall (A,B) \in \mathbb{K}[X]^2,\ A \mid B \iff B\mathbb{K}[X] \subset A\mathbb{K}[X]. \tag{i}$$

$$\forall (A,B) \in \left(\mathbb{K}[X]\backslash\{0\}\right)^2,\ A\mathbb{K}[X] = B\mathbb{K}[X] \iff A \text{ et } B \text{ associés} \iff A^* = B^*. \tag{ii}$$

Théorème 15.37 (Division euclidienne)**.** $(A,B) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$.

$$\exists !(Q,R) \in \mathbb{K}[X]^2,\ A = BQ + R \text{ et } \deg R < \deg B.$$

Démonstration. Existence par récurrence. $\mathcal{P}(n)$: $\forall A \in \mathbb{K}_n[X]$, $\exists (Q,R) \in \mathbb{K}[X]^2$, $A = BQ + R$ et $\deg R < \deg B$. Vérifier d'abord $\mathcal{P}(\deg B - 1)$. Supposer ensuite $\mathcal{P}(n)$ vraie et considérer un polynôme $A \in \mathbb{K}[X]$ t.q. $\deg A = n+1$. En notant a le coefficient dominant de A, b le coefficient dominant de B et $p = \deg B$, poser $A' = A - \frac{a}{b}BX^{n+1-p}$. Vérifier que $\deg A' \leqslant n$ et utiliser $\mathcal{P}(n)$ pour écrire $A' = Q'B + R$, avec $\deg R < \deg B$ puis $A = \left(\frac{a}{b}X^{n+1-p} + Q'\right)B + R$. D'où $\mathcal{P}(n+1)$. Unicité. Supposer $A = BQ_1 + R_1 = BQ_2 + R_2$, avec $\deg R_1 < \deg B$, $\deg R_2 < \deg B$. Écrire $B(Q_1 - Q_2) = R_2 - R_1$. Or $\deg(R_2 - R_1) \leqslant \max(\deg R_1, \deg R_2) < \deg B$, d'où $\deg B + \deg(Q_1 - Q_2) < \deg B$, ou encore $\deg(Q_1 - Q_2) < 0$, donc $\deg(Q_1 - Q_2) = -\infty$, i.e. $Q_1 = Q_2$ et $R_1 = R_2$. □

Corollaire 15.38. $\mathbb{K}[X]$ *est principal.*

Démonstration. Soit I un idéal de $\mathbb{K}[X]$. Poser $\mathcal{H} = \{\deg P,\ P \in I\backslash\{0\}\}$. Montrer que $\mathcal{H}$ admet un plus petit élément d_0 puis choisir $P_0 \in I$ de degré d_0. Montrer alors grâce à la division euclidienne que $I \subset P_0\mathbb{K}[X]$ (l'inclusion réciproque est claire). □

IV Arithmétique dans $\mathbb{K}[X]$

IV.1 Congruences

Définition 15.39 (Congruences)**.** $A \in \mathbb{K}[X]\backslash\{0\}$. *On définit la relation de* congruence modulo A *sur* $\mathbb{K}[X]$ *par* $P \equiv Q \quad [A]$ ssi $(P - Q) \in A\mathbb{K}[X]$.

Proposition 15.40. *La congruence modulo A est une relation d'équivalence sur $\mathbb{K}[X]$, compatible avec $+$ et $\times$:*

$$\forall (P,Q,R,S) \in \mathbb{K}[X]^4,\quad \left.\begin{array}{ll} P \equiv Q & [A] \\ R \equiv S & [A] \end{array}\right\} \Longrightarrow \left\{\begin{array}{ll} P + R \equiv Q + S & [A] \\ P \times R \equiv Q \times S & [A] \end{array}\right. .$$

IV.2 PGCD

Définition 15.41 (PGCD)**.** $(A,B) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$. *On appelle un* PGCD *de A et B tout polynôme de degré maximal divisant A et B.*

Lemme 15.42. $(A,B) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$. *On pose $A = BQ + R$, avec $(Q,R) \in \mathbb{K}[X]^2$,* $\deg R < \deg B$. *Alors les* PGCD *de A et B sont les* PGCD *de B et R.*

Théorème 15.43 (Algorithme d'Euclide)**.** $(A,B) \in \left(\mathbb{K}[X]\backslash\{0\}\right)^2$, $\deg A \geqslant \deg B$. *On note $R_0 = A$, $R_1 = B$. Tant que $R_0, \ldots, R_{n+1}$ sont tous non nuls, on pose $R_n = R_{n+1}Q_{n+1} + R_{n+2}$, avec $(Q_{n+1}, R_{n+2}) \in \mathbb{K}[X]^2$ et* $\deg R_{n+2} < \deg R_{n+1}$. *Alors il existe $N \in \mathbb{N}$ choisi minimal t.q. $R_{N+1} = 0$, et R_N est un* PGCD *de A et B.*

Démonstration. Même démonstration que dans $\mathbb{Z}$ (voir théorème 13.23). □

Théorème 15.44 (Égalité de Bézout)**.** $(A, B) \in (\mathbb{K}[X]\backslash\{0\})^2$*,* Δ *un* PGCD *de* A *et* B*.*

$$\exists (U, V) \in \mathbb{K}[X]^2,\ AU + BV = \Delta.$$

Démonstration. Même démonstration que dans $\mathbb{Z}$ (voir théorème 13.27). □

Proposition 15.45. $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$*.*

(i) *L'ensemble des diviseurs communs de* A *et* B *est l'ensemble des diviseurs d'un* PGCD *de* A *et* B*.*

(ii) *Tous les* PGCD *de* A *et* B *sont associés.*

Définition 15.46 (PGCD)**.** $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$*. Il existe un unique* PGCD *unitaire de* A *et* B*, dit* le PGCD *de* A *et* B*, et noté* $A \wedge B$*.*

Proposition 15.47. $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$*.*

$$A\mathbb{K}[X] + B\mathbb{K}[X] = (A \wedge B)\mathbb{K}[X].$$

Corollaire 15.48. $(A, B, C) \in \mathbb{K}[X] \times (\mathbb{K}[X]\backslash\{0\})^2$*.* $(CA) \wedge (CB) = C^*(A \wedge B)$*.*

IV.3 PPCM

Définition 15.49 (PPCM)**.** $(A, B) \in (\mathbb{K}[X]\backslash\{0\})^2$*. On appelle un* PPCM *de* A *et* B *tout polynôme non nul de degré minimal multiple de* A *et de* B*.*

Proposition 15.50. $(A, B) \in (\mathbb{K}[X]\backslash\{0\})^2$*. Tous les* PPCM *de* A *et* B *sont associés.*

Définition 15.51 (PPCM)**.** $(A, B) \in (\mathbb{K}[X]\backslash\{0\})^2$*. Il existe un unique* PPCM *unitaire de* A *et* B*, dit* le PPCM *de* A *et* B*, et noté* $A \vee B$*.*

Proposition 15.52. $(A, B) \in (\mathbb{K}[X]\backslash\{0\})^2$*.*

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = (A \vee B)\mathbb{K}[X].$$

Corollaire 15.53. $(A, B, C) \in (\mathbb{K}[X]\backslash\{0\})^3$*.* $(CA) \vee (CB) = C^*(A \vee B)$*.*

IV.4 Polynômes premiers entre eux

Définition 15.54 (Polynômes premiers entre eux)**.** $(A, B) \in (\mathbb{K}[X]\backslash\{0\})^2$*. On dit que* A *et* B *sont* premiers entre eux *lorsque* $A \wedge B = 1$*.*

Lemme 15.55 (Lemme de Gauss)**.** $(A, B, C) \in (\mathbb{K}[X]\backslash\{0\})^3$*. Si* $A \mid BC$ *et* $A \wedge B = 1$*, alors* $A \mid C$*.*

Théorème 15.56 (Égalité de Bézout)**.** $(A, B) \in (\mathbb{K}[X]\backslash\{0\})^2$*.*

$$A \wedge B = 1 \iff \exists (U, V) \in \mathbb{K}[X]^2,\ AU + BV = 1.$$

De plus, dans ce cas et à condition que $\deg A \geqslant 1$*,* $\deg B \geqslant 1$*, il existe un unique polynôme* U *t.q.* $\deg U < \deg B$*, et on a alors* $\deg V < \deg A$*.*

Démonstration. L'implication ($\Rightarrow$) découle du théorème 15.44, l'autre est facile à démontrer. Existence de U et V vérifiant $\deg U < \deg B$, $\deg V < \deg A$. Supposer $A \wedge B = 1$. Soit $(U_0, V_0) \in \mathbb{K}[X]^2$ t.q. $AU_0 + BV_0 = 1$. On a alors $AU + BV = 1 \iff A(U - U_0) = B(V_0 - V)$. Supposer (U, V) solution, utiliser le lemme 15.55 pour en déduire que $A \mid V_0 - V$. Donc $(U, V) = (U_0 + QB, V_0 - QA)$, avec $Q \in \mathbb{K}[X]$. Vérifier réciproquement que ces couples conviennent. Utiliser alors la division euclidienne : $U_0 = QB + R$, $(Q, R) \in \mathbb{K}[X]^2$ et $\deg R < \deg B$. Choisir $U = R$, $V = V_0 + QA$, et vérifier que U et V conviennent (ils sont solutions de $AU + BV = 1$ et $\deg U < \deg B$, $\deg V < \deg A$). Montrer l'unicité de manière classique. □

Proposition 15.57. $(A, B, C) \in (\mathbb{K}[X]\backslash\{0\})^3$. $(P_1, \ldots, P_n) \in (\mathbb{K}[X]\backslash\{0\})^n$.

$$A \wedge \left(\prod_{i=1}^{n} P_i \right) = 1 \iff \forall i \in [\![1, n]\!],\ A \wedge P_i = 1. \tag{i}$$

$$A \wedge B = 1 \Longrightarrow \forall (k, \ell) \in (\mathbb{N}^*)^2,\ A^k \wedge B^\ell = 1. \tag{ii}$$

$$\left.\begin{array}{r} B \mid A \\ C \mid A \\ B \wedge C = 1 \end{array}\right\} \Longrightarrow BC \mid A. \tag{iii}$$

$$\exists (A_1, A_2) \in \mathbb{K}[X]^2,\ \left\{\begin{array}{l} A = (A \wedge B)A_1 \\ B = (A \wedge B)B_1 \\ A_1 \wedge B_1 = 1 \end{array}\right. . \tag{iv}$$

$$(A \wedge B)(A \vee B) = A^* B^*. \tag{v}$$

IV.5 PGCD et PPCM de n polynômes

Définition 15.58 (PGCD)**.** $(A_1, \ldots, A_n) \in (\mathbb{K}[X]\backslash\{0\})^n$. *On appelle* PGCD *de* $A_1, \ldots, A_n$ *tout polynôme de degré maximal divisant chacun des* A_i, $i \in [\![1, n]\!]$.

Définition 15.59 (PPCM)**.** $(A_1, \ldots, A_n) \in (\mathbb{K}[X]\backslash\{0\})^n$. *On appelle* PPCM *de* $A_1, \ldots, A_n$ *tout polynôme non nul de degré minimal multiple de chacun des* A_i, $i \in [\![1, n]\!]$.

Proposition 15.60. $(A_1, \ldots, A_n) \in (\mathbb{K}[X]\backslash\{0\})^n$. $P \in \mathbb{K}[X]$.

$$\forall i \in [\![1, n]\!],\ P \mid A_i \iff P \text{ divise un PGCD de } A_1, \ldots, A_n. \tag{i}$$

$$\forall i \in [\![1, n]\!],\ A_i \mid P \iff P \text{ est multiple d'un PPCM de } A_1, \ldots, A_n. \tag{ii}$$

Corollaire 15.61. *Tous les* PGCD *(resp.* PPCM*) de n polynômes non nuls sont associés.*

Notation 15.62. $(A_1, \ldots, A_n) \in (\mathbb{K}[X]\backslash\{0\})^n$. *On note* $A_1 \wedge \cdots \wedge A_n$ *l'unique* PGCD *unitaire de* $A_1, \ldots, A_n$. *On note* $A_1 \vee \cdots \vee A_n$ *l'unique* PPCM *unitaire de* $A_1, \ldots, A_n$.

Proposition 15.63. $(A, B, C) \in (\mathbb{K}[X]\backslash\{0\})^3$.

$$(A \wedge B) \wedge C = A \wedge B \wedge C. \tag{i}$$

$$A\mathbb{K}[X] + B\mathbb{K}[X] + C\mathbb{K}[X] = (A \wedge B \wedge C)\mathbb{K}[X]. \tag{ii}$$

Proposition 15.64. $(A_1, \ldots, A_n) \in (\mathbb{K}[X]\backslash\{0\})^n$. *On suppose que* $\forall (i, j) \in [\![1, n]\!]^2$, $i \neq j \Rightarrow A_i \wedge A_j = 1$. *Alors* $A_1 \vee \cdots \vee A_n = \prod_{i=1}^{n} A_i^*$.

V Fonctions polynomiales

V.1 Généralités

Définition 15.65 (Fonction polynomiale)**.** $P = \sum_{k\in\mathbb{N}} \lambda_k X^k \in \mathbb{K}[X]$. *On appelle* fonction polynomiale associée à P *la fonction*

$$\widetilde{P} : \left| \begin{array}{l} \mathbb{K} \longrightarrow \mathbb{K} \\ x \longmapsto \displaystyle\sum_{k\in\mathbb{N}} \lambda_k x^k \end{array} \right. .$$

Proposition 15.66. *L'application* $\psi : \mathbb{K}[X] \longrightarrow \mathbb{K}^{\mathbb{K}}$ *définie par* $\psi : P \longmapsto \widetilde{P}$ *est un morphisme d'anneau et on a de plus* $\forall(\lambda, P) \in \mathbb{K}\times\mathbb{K}[X], \widetilde{\lambda P} = \lambda\widetilde{P}$ *et* $\forall(P, Q) \in \mathbb{K}[X]^2, \widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.

Notation 15.67. $P = \sum_{k\in\mathbb{N}} \lambda_k X^k \in \mathbb{C}[X]$. *On définit*

$$\overline{P} = \sum_{k\in\mathbb{N}} \overline{\lambda_k} X^k.$$

Proposition 15.68. *L'application* $\psi : \mathbb{C}[X] \longrightarrow \mathbb{C}[X]$ *définie par* $\psi : P \longmapsto \overline{P}$ *est un morphisme d'anneau et on a de plus* $\forall(\lambda, P) \in \mathbb{K} \times \mathbb{K}[X]$, $\overline{\lambda P} = \overline{\lambda} \cdot \overline{P}$ *et* $\forall(P, Q) \in \mathbb{K}[X]^2$, $\overline{P \circ Q} = \overline{P} \circ \overline{Q}$.

Proposition 15.69. $\forall P \in \mathbb{C}[X]$, $\widetilde{\overline{P}} = \overline{\widetilde{P}}$.

V.2 Racines d'un polynôme

Définition 15.70 (Racine d'un polynôme)**.** $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$. *On dit que* a *est* racine *de* P *lorsque* $\widetilde{P}(a) = 0$.

Lemme 15.71. $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$. *Le reste de la division euclidienne de* P *par* $X - a$ *est* $\widetilde{P}(a)X^0$.

Proposition 15.72. $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$. a *est racine de* P ssi $X - a \mid P$.

Définition 15.73 (Multiplicité d'une racine)**.** $P \in \mathbb{K}[X]\backslash\{0\}$, $a \in \mathbb{K}$, $m \in \mathbb{N}$. *On dit que* a *racine de* P *est de* multiplicité m *lorsque* $(X - a)^m \mid P$ *et* $(X - a)^{m+1} \nmid P$. *On dit que* a *est de multiplicité* 0 *lorsque* a *non racine de* P.

Vocabulaire 15.74. $P \in \mathbb{K}[X]\backslash\{0\}$, $a \in \mathbb{K}$. *Si* a *est de multiplicité* 1, a *est dit* racine simple *; si* a *est de multiplicité strictement supérieure à* 1, a *est dit* racine multiple.

Proposition 15.75. $P \in \mathbb{K}[X]\backslash\{0\}$, $a \in \mathbb{K}$, $m \in \mathbb{N}$.

$$a \text{ racine de multiplicité } m \text{ de } P \Longleftrightarrow \exists Q \in \mathbb{K}[X], \left\{ \begin{array}{l} P = Q(X - a)^m \\ \widetilde{Q}(a) \neq 0 \end{array} \right. .$$

Proposition 15.76. $P \in \mathbb{C}[X]\backslash\{0\}$, $a \in \mathbb{C}$, $m \in \mathbb{N}$. a *est racine de multiplicité* m *de* P ssi $\overline{a}$ *est racine de multiplicité* m *de* $\overline{P}$.

V.3 Nombre de racines d'un polynôme

Proposition 15.77. *$P \in \mathbb{K}[X]\backslash\{0\}$, $(a_1, \dots, a_r) \in \mathbb{K}^r$, $(m_1, \dots, m_r) \in (\mathbb{N}^*)^r$, avec $a_1 < \dots < a_r$.*

$\forall i \in [\![1, r]\!]$, a_i racine de multiplicité m_i de P

$$\iff \exists Q \in \mathbb{K}[X],\ \begin{cases} P = Q\prod_{i=1}^r (X-a_i)^{m_i} \\ \forall i \in [\![1,r]\!],\ \widetilde{Q}(a_i) \neq 0 \end{cases}.$$

Vocabulaire 15.78. *$P = Q\prod_{i=1}^r (X-a_i)^{m_i} \in \mathbb{K}[X]\backslash\{0\}$, avec $(a_1, \dots, a_r) \in \mathbb{K}^r$, $(m_1, \dots, m_r) \in (\mathbb{N}^*)^r$ et $Q \in \mathbb{K}[X]$, où Q n'admet aucune racine dans $\mathbb{K}$. Alors on dit que P a $\sum_{i=1}^r m_i$* racines comptées avec leur multiplicité. *Si de plus $\deg Q = 0$, on dit que P est* scindé sur $\mathbb{K}$.

Proposition 15.79. *$P \in \mathbb{K}[X]\backslash\{0\}$. P possède au plus $\deg P$ racines comptées avec leur multiplicité.*

Corollaire 15.80. *$(x_0, \dots, x_n) \in \mathbb{K}^{n+1}$, $(y_0, \dots, y_n) \in \mathbb{K}^{n+1}$, avec $x_0 < \dots < x_n$. On suppose ici $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.*

$$\exists! P \in \mathbb{K}_n[X],\ \forall i \in [\![0, n]\!],\ \widetilde{P}(x_i) = y_i.$$

Démonstration. Existence. Poser $P = \sum_{i=0}^n y_i L_i$, avec $L_i = \dfrac{\prod_{j\neq i}(X-x_j)}{\prod_{j\neq i}(x_i-x_j)}$. Vérifier que P convient. Unicité. Utiliser la contraposée de la proposition 15.79. □

V.4 Identification entre fonctions polynomiales et polynômes

Proposition 15.81. *Le morphisme d'anneaux $\psi : \mathbb{K}[X] \longrightarrow \mathbb{K}^{\mathbb{K}}$ défini par $\psi : P \longmapsto \widetilde{P}$ est injectif.*

V.5 Relation entre coefficients et racines

Définition 15.82 (Fonctions symétriques)**.** *$(\lambda_1, \dots, \lambda_p) \in \mathbb{K}^p$. On définit les* fonctions symétriques élémentaires *$\sigma_1, \dots, \sigma_p$ de $\lambda_1, \dots, \lambda_p$ par :*

$$\forall k \in [\![1, p]\!],\ \sigma_k = \sum_{1\leqslant i_1 < \dots < i_k \leqslant p} \lambda_{i_1} \cdots \lambda_{i_k}.$$

Proposition 15.83. *$P \in \mathbb{K}[X]\backslash\{0\}$ scindé sur $\mathbb{K}$. On suppose $P = \eta\prod_{i=1}^r (X-a_i)^{m_i} = \sum_{k\in\mathbb{N}} \lambda_k X^k$. On note $p = \deg P$.*

$$\forall k \in [\![1, p]\!],\ \lambda_{p-k} = (-1)^k \lambda_p \sigma_k.$$

VI Dérivation

VI.1 Généralités

Définition 15.84 (Dérivée d'un polynôme)**.** *$P = \sum_{k\in\mathbb{N}} \lambda_k X^k \in \mathbb{K}[X]$. On définit la* dérivée de P *comme étant le polynôme*

$$P' = \sum_{k\in\mathbb{N}^*} k\lambda_k X^{k-1}.$$

On définit de plus par récurrence les dérivées successives de P : $P^{(0)} = P$ et $\forall j \in \mathbb{N}$, $P^{(j+1)} = \left(P^{(j)}\right)'$.

Proposition 15.85.

$$\forall P \in \mathbb{K}[X],\ P' = 0 \iff P \text{ polynôme constant.} \tag{i}$$

$$\forall P \in \mathbb{K}[X],\ \forall j \in [\![0, \deg P]\!],\ \deg P^{(j)} = \deg P - j. \tag{ii}$$

$$\forall P \in \mathbb{K}[X]\backslash\{0\},\ P^{(1+\deg P)} = 0. \tag{iii}$$

$$\forall (P, Q, \lambda) \in \mathbb{K}[X]^2 \times \mathbb{K},\ \begin{cases} (P+Q)' = P' + Q' \\ (PQ)' = P'Q + PQ' \\ (\lambda P)' = \lambda P' \\ (P \circ Q)' = Q' \cdot (P' \circ Q) \end{cases}. \tag{iv}$$

$$\forall P \in \mathbb{R}[X],\ \widetilde{P'} = \left(\widetilde{P}\right)'. \tag{v}$$

$$\forall P \in \mathbb{C}[X],\ \overline{P'} = \left(\overline{P}\right)'. \tag{vi}$$

Théorème 15.86 (Formule de Leibniz)**.** $(P, Q) \in \mathbb{K}[X]^2$, $n \in \mathbb{N}$.

$$(PQ)^{(n)} = \sum_{k \in \mathbb{N}} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

VI.2 Formule de Taylor et conséquences

Proposition 15.87. $P \in \mathbb{K}[X]\backslash\{0\}$, $a \in \mathbb{K}$.

$$P = \sum_{k=0}^{\deg P} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k.$$

Démonstration. Supposer d'abord $a = 0$ et montrer l'égalité voulue. Pour $a \in \mathbb{K}$ quelconque, poser $Q = P \circ (X+a)$. Utiliser la première étape pour écrire $Q = \sum_{k=0}^{\deg Q} \frac{\widetilde{Q^{(k)}}(0)}{k!} X^k$, puis en déduire l'égalité souhaitée en utilisant $P = Q \circ (X-a)$. □

Remarque 15.88. *On sait que tout polynôme $P \in \mathbb{K}[X]$ s'écrit sous la forme $P = \sum_{k \in \mathbb{N}} \lambda_k X^k$ de manière unique. De plus, pour tout $a \in \mathbb{K}$, P peut s'écrire sous la forme $P = \sum_{k \in \mathbb{N}} \mu_k (X-a)^k$ de manière unique.*

Lemme 15.89. *$P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $m \in \mathbb{N}^*$. Le reste de la division euclidienne de P par $(X-a)^m$ est $\sum_{k=0}^{m-1} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k$.*

Proposition 15.90. $P \in \mathbb{K}[X]\backslash\{0\}$, $a \in \mathbb{K}$, $m \in \mathbb{N}^*$.

a racine de multiplicité m de P

$$\iff \begin{cases} \forall k \in [\![0, m-1]\!],\ \widetilde{P^{(k)}}(a) = 0 \\ \widetilde{P^{(m)}}(a) \neq 0 \end{cases}, \tag{i}$$

$$\iff \text{a racine de multiplicité } (m-1) \text{ de } P'. \tag{ii}$$

$$a \text{ racine multiple de } P \iff \widetilde{P'}(a) = \widetilde{P}(a) = 0. \tag{iii}$$

VII Polynômes irréductibles

VII.1 Généralités

Définition 15.91 (Polynôme irréductible)**.** $P \in \mathbb{K}[X]\backslash\mathbb{K}_0[X]$. *$P$ est dit* irréductible *dans* $\mathbb{K}[X]$ *lorsque*

$$\forall (Q,H) \in \mathbb{K}[X]^2,\ P = QH \Longrightarrow Q \text{ constant ou } H \text{ constant.}$$

Proposition 15.92. $P \in \mathbb{K}[X]\backslash\mathbb{K}_0[X]$.

$$\deg P = 1 \Longrightarrow P \text{ irréductible.} \tag{i}$$

$$\deg P \geqslant 2 \text{ et } P \text{ admet une racine dans } \mathbb{K} \Longrightarrow P \text{ non irréductible.} \tag{ii}$$

Proposition 15.93. $P \in \mathbb{K}[X]\backslash\mathbb{K}_0[X]$ *irréductible.*

$$\forall A \in \mathbb{K}[X],\ P \mid A \text{ ou } P \wedge A = 1. \tag{i}$$

$$\forall (A_1,\dots,A_n) \in \mathbb{K}[X]^n,\ P \mid \left(\prod_{i=1}^{n} A_i\right) \Longleftrightarrow \exists i \in [\![1,n]\!],\ P \mid A_i. \tag{ii}$$

Définition 15.94 (Valuation P-adique)**.** $P \in \mathbb{K}[X]\backslash\mathbb{K}_0[X]$ *irréductible.* $A \in \mathbb{K}[X]\backslash\{0\}$. *On appelle* valuation P-adique de A *l'entier*

$$v_P(A) = \max\{k \in \mathbb{N},\ P^k \mid A\}.$$

Lemme 15.95. $P \in \mathbb{K}[X]\backslash\mathbb{K}_0[X]$ *irréductible.* $(A,B) \in (\mathbb{K}[X]\backslash\{0\})^2$. *Alors* $v_P(AB) = v_P(A) + v_P(B)$.

Proposition 15.96. $P \in \mathbb{K}[X]\backslash\mathbb{K}_0[X]$ *irréductible.* $(A,B) \in (\mathbb{K}[X]\backslash\{0\})^2$.

$$A \mid B \Longrightarrow v_P(A) \leqslant v_P(B).$$

VII.2 Décomposition d'un polynôme

Proposition 15.97.

$\forall A \in \mathbb{K}[X]\backslash\mathbb{K}_0[X],\ \exists (P_1,\dots,P_r) \in \mathbb{K}[X]^r$ *irréductibles unitaires,*

$$\exists (\alpha_1,\dots,\alpha_r) \in (\mathbb{N}^*)^r,\ \exists \lambda \in \mathbb{K}^*,\ A = \lambda \prod_{i=1}^{r} P_i^{\alpha_i}.$$

De plus, cette écriture est unique à l'ordre près des facteurs (en supposant $\forall (i,j) \in [\![1,r]\!]^2,\ i \neq j \Longrightarrow P_i \neq P_j$*).*

Démonstration. Existence. Par récurrence forte. Unicité. Supposer $A = \prod_{i=1}^{r} P_i^{\alpha_i} = \prod_{i=1}^{s} Q_i^{\beta_i}$. Montrer que $\forall i \in [\![1,r]\!],\ \exists j \in [\![1,s]\!],\ P_i = Q_j$, et inversement. En déduire que $\{P_1,\dots,P_r\} = \{Q_1,\dots,Q_s\}$. Montrer ensuite que $\forall i \in [\![1,r]\!],\ \alpha_i = v_{P_i}(A)$ et $\forall j \in [\![1,s]\!],\ \beta_i = v_{Q_i}(A)$. D'où l'unicité de l'écriture. □

Proposition 15.98. $(A,B) \in (\mathbb{K}[X]\backslash\{0\})^2$. *On écrit* $A = \lambda \prod_{i=1}^{r} P_i^{\alpha_i}$, $B = \mu \prod_{i=1}^{r} P_i^{\beta_i}$, *avec* $(P_1,\dots,P_r) \in \mathbb{K}[X]^r$ *irréductibles unitaires,* $(\alpha_1,\dots,\alpha_r) \in \mathbb{N}^r$, $(\beta_1,\dots,\beta_r) \in \mathbb{N}^r$, $(\lambda,\mu) \in (\mathbb{K}^*)^2$.

$$A \mid B \Longleftrightarrow \forall i \in [\![1,r]\!],\ \alpha_i \leqslant \beta_i, \tag{i}$$

$$A \wedge B = \prod_{i=1}^{r} P_i^{\min(\alpha_i,\beta_i)}, \tag{ii}$$

$$A \vee B = \prod_{i=1}^{r} P_i^{\max(\alpha_i,\beta_i)}. \tag{iii}$$

VII.3 Décomposition dans $\mathbb{C}[X]$

Théorème 15.99 (Théorème de d'Alembert-Gauss)**.** *Tout polynôme non constant de* $\mathbb{C}[X]$ *admet au moins une racine dans* $\mathbb{C}$*.*

Corollaire 15.100. *Tout polynôme non constant dans* $\mathbb{C}[X]$ *est scindé dans* $\mathbb{C}[X]$*.*

Démonstration. Par récurrence sur le degré. □

Proposition 15.101. *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré* 1*.*

VII.4 Décomposition dans $\mathbb{R}[X]$

Proposition 15.102. $P \in \mathbb{K}[X] \backslash \mathbb{K}_0[X]$*.* P *est scindé* ssi *le degré de* P *est égal au nombre de racines de* P *comptées avec leur multiplicité.*

Proposition 15.103. *Les polynômes irréductibles dans* $\mathbb{R}[X]$ *sont les polynômes de degré* 1 *et les polynômes de degré* 2 *sans racines réelles.*

Démonstration. Montrer d'abord que les polynômes de degré 1 et les polynômes de degré 2 sans racines réelles sont irréductibles dans $\mathbb{R}[X]$. Réciproquement, prendre un polynôme P t.q. $\deg P \geqslant 3$ (si $\deg P = 2$ et P admet une racine réelle, P n'est clairement pas irréductible). P admet une racine complexe α d'après le théorème 15.99. Si $\alpha \in \mathbb{R}$, factoriser P par $(X - \alpha) \in \mathbb{R}[X]$, sinon $\overline{\alpha}$ est aussi racine et on peut factoriser P par $(X - \alpha)(X - \overline{\alpha}) \in \mathbb{R}[X]$. Donc P n'est pas irréductible. □

Chapitre 16

Fractions Rationnelles

I Généralités

Notation 16.1. *Soit $\mathcal{R}$ la relation définie sur $\mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$ par*

$$(A, B)\mathcal{R}(C, D) \iff AD = BC.$$

Proposition 16.2. *$\mathcal{R}$ est une relation d'équivalence.*

Définition 16.3 (Fraction rationnelle)**.** *Pour $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$, on note $\frac{A}{B}$ la classe d'équivalence de (A, B), dite* fraction rationnelle*. L'ensemble des fractions rationnelles est noté $\mathbb{K}(X)$.*

Remarque 16.4. *On dit que $\mathbb{K}[X] \subset \mathbb{K}(X)$ au sens où il existe une injection $\mathbb{K}[X] \to \mathbb{K}(X)$.*

Définition 16.5 (LCI sur $\mathbb{K}(X)$)**.** *Pour $\left(\frac{A}{B}, \frac{C}{D}\right) \in \mathbb{K}(X)^2$, on définit les LCI $+$ et $\times$ par :*

$$\frac{A}{B} + \frac{C}{D} = \frac{AD + BC}{BD} \qquad et \qquad \frac{A}{B} \times \frac{C}{D} = \frac{AC}{BD}.$$

Proposition 16.6. *$(\mathbb{K}(X), +, \times)$ est un corps.*

Proposition 16.7 (Écriture normalisée)**.** *$F \in \mathbb{K}(X)\backslash\{0\}$.*

$$\exists!(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}, \begin{cases} P \wedge Q = 1 \\ Q \text{ unitaire} \\ F = \frac{P}{Q} \end{cases}.$$

On dit que $\frac{P}{Q}$ est un représentant irréductible et normalisé *de F.*

Définition 16.8 (Composition)**.** *Pour $\frac{A}{B} \in \mathbb{K}(X)$, $P \in \mathbb{K}[X]\backslash\mathbb{K}_0[X]$, on définit*

$$\frac{A}{B} \circ P = \frac{A \circ P}{B \circ P}.$$

Définition 16.9 (Parité)**.** *$F \in \mathbb{K}(X)$. On dit que F est* paire *lorsque $F \circ (-X) = F$; on dit que F est* impaire *lorsque $F \circ (-X) = -F$.*

Notation 16.10. $\frac{A}{B} \in \mathbb{C}(X)$. *On définit*

$$\overline{\left(\frac{A}{B}\right)} = \frac{\overline{A}}{\overline{B}}.$$

Proposition 16.11. *L'application* $\left|\begin{array}{c}\mathbb{C}(X) \longrightarrow \mathbb{C}(X) \\ F \longmapsto \overline{F}\end{array}\right.$ *est un automorphisme de corps.*

Proposition 16.12. $\forall F \in \mathbb{C}(X),\ F \in \mathbb{R}(X) \iff F = \overline{F}$.

II Degré, dérivation et racines

II.1 Degré

Définition 16.13 (Degré)**.** $\frac{A}{B} \in \mathbb{K}(X)$. *On définit* $\deg \frac{A}{B} = \deg A - \deg B$.

Proposition 16.14. $(F, G) \in \mathbb{K}(X)^2$.

$$\deg F = -\infty \iff F = 0, \tag{i}$$

$$\deg(F+G) \leqslant \max(\deg F, \deg G) \quad \textit{avec égalité dès que } \deg F \neq \deg G, \tag{ii}$$

$$\deg(FG) = \deg F + \deg G. \tag{iii}$$

II.2 Dérivation

Définition 16.15 (Dérivée d'une fraction rationnelle)**.** $\frac{A}{B} \in \mathbb{K}(X)$. *On définit la* dérivée de $\frac{A}{B}$ *comme étant la fraction rationnelle*

$$\left(\frac{A}{B}\right)' = \frac{A'B - AB'}{B^2}.$$

On définit de plus par récurrence les dérivées successives de $\frac{A}{B}$ *:* $\left(\frac{A}{B}\right)^{(0)} = \frac{A}{B}$ *et* $\forall j \in \mathbb{N},\ \left(\frac{A}{B}\right)^{(j+1)} = \left(\left(\frac{A}{B}\right)^{(j)}\right)'$.

Proposition 16.16. $(F, G) \in \mathbb{K}(X)^2,\ \lambda \in \mathbb{K}$.

$$(F+G)' = F' + G' \quad et \quad (\lambda F)' = \lambda F' \quad et \quad (FG)' = F'G + FG'.$$

II.3 Fonctions rationnelles

Définition 16.17 (Fonction rationnelle)**.** $\frac{A}{B} \in \mathbb{K}(X)$. *On appelle* fonction rationnelle associée à $\frac{A}{B}$ *la fonction*

$$\widetilde{\left(\frac{A}{B}\right)} : \left|\begin{array}{c}\mathbb{K}\backslash\mathscr{R} \longrightarrow \mathbb{K} \\ x \longmapsto \dfrac{\widetilde{A}(x)}{\widetilde{B}(x)}\end{array}\right. ,$$

avec $\mathscr{R} = \left\{\rho \in \mathbb{K},\ \widetilde{B}(\rho) = 0\right\}$.

Proposition 16.18. $(F, G) \in \mathbb{K}(X)^2,\ \lambda \in \mathbb{K}$.

$$\widetilde{F+G} = \widetilde{F} + \widetilde{G} \quad et \quad \widetilde{\lambda F} = \lambda \widetilde{F} \quad et \quad \widetilde{FG} = \widetilde{F}\widetilde{G}.$$

Proposition 16.19. $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. $(F, G) \in \mathbb{K}(X)^2$. *Si* $\widetilde{F}$ *et* $\widetilde{G}$ *sont égales en un nombre infini de points, alors* $F = G$.

II.4 Racines et pôles d'une fraction rationnelle

Définition 16.20 (Racines et pôles d'une fraction rationnelle)**.** $\frac{A}{B} \in \mathbb{K}(X)$. *On appelle* racine *de* $\frac{A}{B}$ *de multiplicité* m *toute racine de* A *de multiplicité* m *; on appelle* pôle *de* $\frac{A}{B}$ *de multiplicité* m *toute racine de* B *de multiplicité* m.

Proposition 16.21. $F \in \mathbb{K}(X)$, $\alpha \in \mathbb{K}$. α *racine de* $F \iff \widetilde{F}(\alpha) = 0$.

III Décomposition d'une fraction rationnelle en éléments simples dans $\mathbb{K}(X)$

III.1 Partie entière

Proposition 16.22 (Partie entière d'une fraction rationnelle)**.** $F \in \mathbb{K}(X)$.

$$\exists!(E_F, G) \in \mathbb{K}[X] \times \mathbb{K}(X),\ F = E_F + G \text{ et } \deg G < 0.$$

E_F *est dite* partie entière *de* F.

Démonstration. Avec $F = \frac{A}{B}$, écrire la division euclidienne de A par B. □

Proposition 16.23. $F = \frac{A}{B} \in \mathbb{K}(X)$. *On note* E_F *la partie entière de* F.

$$\deg A < \deg B \Longrightarrow E_F = 0. \tag{i}$$

$$\deg A = \deg B \Longrightarrow E_F = \frac{a}{b}, \tag{ii}$$

où a *et* b *sont les coefficients dominants respectifs de* A *et* B.

Proposition 16.24. $\forall (F, G) \in \mathbb{K}(X)^2,\ \forall (\lambda, \mu) \in \mathbb{K}^2,\ E_{\lambda F + \mu G} = \lambda E_F + \mu E_G$.

III.2 Décomposition d'une fraction rationnelle

Définition 16.25 (Décomposition en éléments simples)**.** $F = \frac{A}{B} \in \mathbb{K}(X)$, *avec* B *unitaire. On écrit* $B = \prod_{i=1}^{r} P_i^{\alpha_i}$, *avec* $(P_1, \dots, P_r) \in \mathbb{K}[X]^r$ *irréductibles unitaires deux à deux distincts,* $(\alpha_1, \dots, \alpha_r) \in (\mathbb{N}^*)^r$. *Alors toute écriture de la forme*

$$F = \underbrace{E_F}_{\substack{\text{partie} \\ \text{entière de } F}} + \sum_{i=1}^{r} \underbrace{\sum_{j=1}^{\alpha_i} \frac{V_{i,j}}{P_i^j}}_{\substack{\text{partie polaire} \\ \text{associée à } P_i}},$$

est dite décomposition en éléments simples *de* F *dans* $\mathbb{K}(X)$, *où les* $V_{i,j}$ *sont des polynômes vérifiant* $\deg V_{i,j} < \deg P_i$.

Lemme 16.26. $(P, Q_1, Q_2) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})^2$, *avec* $Q_1 \wedge Q_2 = 1$ *et* $\deg \frac{P}{Q_1 Q_2} < 0$.

$$\exists (U_1, U_2) \in \mathbb{K}[X]^2,\ \frac{P}{Q_1 Q_2} = \frac{U_1}{Q_1} + \frac{U_2}{Q_2} \quad \text{et } \deg U_1 < \deg Q_1 \text{ et } \deg U_2 < \deg Q_2.$$

Démonstration. Utiliser Bézout pour écrire $AQ_1 + BQ_2 = 1$, avec $(A, B) \in \mathbb{K}[X]^2$. En déduire $APQ_1 + BPQ_2 = P$. Écrire la division euclidienne de AP par Q_2 : $AP = WQ_2 + U_2$, avec $\deg U_2 < \deg Q_2$. Poser alors $U_1 = BP + Q_1 W$, puis vérifier que U_1 et U_2 conviennent. □

Lemme 16.27. $(U,Q) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$, $n \in \mathbb{N}^*$ *t.q.* $\deg \frac{U}{Q^n} < 0$.

$$\exists (V_1,\dots,V_n) \in \mathbb{K}[X]^n,\ \frac{U}{Q^n} = \sum_{k=1}^{n} \frac{V_i}{Q^i} \text{ et } \forall i \in [\![1,n]\!],\ \deg V_i < \deg Q.$$

Démonstration. Par division euclidienne de U par Q, écrire $U = QW + V_n$, avec $\deg V_n < \deg Q$, donc $F = \frac{W}{Q^{n-1}} + \frac{V_n}{Q^n}$, et $\deg \frac{W}{Q^{n-1}} < 0$. Justifier alors l'existence de $V_1,\dots,V_n$ par récurrence descendante. □

Proposition 16.28. *Toute fraction rationnelle admet une unique décomposition en éléments simples.*

Démonstration. Existence. Appliquer le lemme 16.26 puis le lemme 16.27. □

IV Détermination des éléments simples

IV.1 Éléments simples associés à $(X-\alpha)$

Proposition 16.29. $F = \frac{A}{(X-\alpha)^n B} \in \mathbb{K}(X)$, *avec* $(A,B) \in \mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$, $\widetilde{A}(\alpha) \neq 0$, $\widetilde{B}(\alpha) \neq 0$, *et* $n \in \mathbb{N}^*$. *Alors*

$$F = E_F + H + \sum_{k=1}^{n} \frac{\lambda_k}{(X-\alpha)^k},$$

où $H \in \mathbb{K}(X)$, $\deg H < 0$, H *n'admet pas* α *pour pôle et*

$$\lambda_n = \frac{\widetilde{A}(\alpha)}{\widetilde{B}(\alpha)} = \frac{n!\widetilde{A}(\alpha)}{\widetilde{C^{(n)}}(\alpha)},$$

avec $C = (X-\alpha)^n B$.

IV.2 Quelques règles en pratique

Méthode 16.30. $F \in \mathbb{K}(X)$. *Pour simplifier la décomposition en éléments simples de* F, *on peut s'appuyer sur les règles suivantes :*

(i) *Si* F *est paire (resp. impaire), on a* $F(X) = F(-X)$ *(resp.* $F(X) = -F(-X)$*), donc on obtient deux décompositions en éléments simples de* F. *Par unicité de la décomposition en éléments simples, on obtient des relations entre les coefficients.*

(ii) *Si* $F \in \mathbb{R}(X)$, *on peut décomposer* F *sur* $\mathbb{C}(X)$ *et utiliser* $\overline{F} = F$.

(iii) *On peut évaluer* $\widetilde{F}$ *en certains points judicieux (y compris en* $\pm\infty$*).*

IV.3 Un exemple important

Proposition 16.31. $P \in \mathbb{K}[X]\backslash\{0\}$ *scindé sur* $\mathbb{K}$, *avec* $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. *On peut alors écrire* $P = \lambda \prod_{k=1}^{n}(X-a_k)$, *avec* $(a_1,\dots,a_n) \in \mathbb{K}^n$, $\lambda \in \mathbb{K}^*$. *On a alors :*

$$\frac{P'}{P} = \sum_{k=1}^{n} \frac{1}{X-a_k}.$$

Chapitre 17

Espaces Vectoriels

I Généralités

I.1 Définition

Définition 17.1 (Espace vectoriel)**.** *E un ensemble, $+$ une LCI sur E, $\cdot$ une LCE $\mathbb{K}\times E \to E$. On dit que $(E,+,\cdot)$ est un* $\mathbb{K}$-espace vectoriel *lorsque :*

(i) $(E,+)$ *est un groupe commutatif.*

(ii) $\forall(\lambda,\mu)\in\mathbb{K}^2,\ \forall(x,y)\in E^2,\ \begin{cases} \lambda\cdot(x+y)=\lambda\cdot x+\lambda\cdot y \\ (\lambda+\mu)\cdot x=\lambda\cdot x+\mu\cdot x \\ (\lambda\times\mu)\cdot x=\lambda\cdot(\mu\cdot x)\end{cases}$.

(iii) $\forall x\in E,\ 1_{\mathbb{K}}\cdot x=x$.

Les éléments de E sont dits vecteurs*, les éléments de $\mathbb{K}$ sont dits* scalaires*.*

Définition 17.2 (Produit cartésien d'espaces vectoriels)**.** *$(E,+_1,\cdot_1)$ et $(F,+_2,\cdot_2)$ deux $\mathbb{K}$-espaces vectoriels. On définit la LCI $+$ sur $E\times F$ par*

$$+ : \left| \begin{array}{l} (E\times F)\times(E\times F)\longrightarrow E\times F \\ ((x_1,x_2),(y_1,y_2))\longmapsto(x_1+_1y_1,x_2+_2y_2)\end{array}\right. .$$

On définit de même la LCE $\cdot$ par

$$\cdot : \left| \begin{array}{l} \mathbb{K}\times(E\times F)\longrightarrow E\times F \\ (\lambda,(x_1,x_2))\longmapsto(\lambda\cdot_1x_1,\lambda\cdot_2y_2)\end{array}\right. .$$

Alors $(E\times F,+,\cdot)$ est un $\mathbb{K}$-espace vectoriel, dit produit cartésien *de E et F.*

Proposition 17.3. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel, A un ensemble non vide. Alors $(E^A,+,\cdot)$ est un $\mathbb{K}$-espace vectoriel.*

Exemple 17.4. *Pour $n\in\mathbb{N}^*$, $(\mathbb{R}^n,+,\cdot)$, est un $\mathbb{R}$-espace vectoriel, $(\mathbb{C}^n,+,\cdot)$ est un $\mathbb{R}$-espace vectoriel et un $\mathbb{C}$-espace vectoriel. $(\mathbb{R}^{\mathbb{R}},+,\cdot)$, $(\mathbb{R}^{\mathbb{N}},+,\cdot)$ sont des $\mathbb{R}$-espaces vectoriels. $(\mathbb{K}(X),+,\cdot)$ est un $\mathbb{K}$-espace vectoriel.*

I.2 Règles de calcul dans un espace vectoriel

Proposition 17.5. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x,y)\in E^2$, $(\lambda,\mu)\in\mathbb{K}^2$.*

(i) $0_{\mathbb{K}}\cdot x = 0_E$,

(ii) $\lambda\cdot 0_E = 0_E$,

(iii) $\lambda\cdot x = 0_E \iff \lambda = 0_{\mathbb{K}}$ ou $x = 0_E$,

(iv) $-(\lambda\cdot x) = (-\lambda)\cdot x$,

(v) $\lambda\cdot(x-y) = \lambda\cdot x - \lambda\cdot y$,

(vi) $(\lambda-\mu)\cdot x = \lambda\cdot x - \mu\cdot x$.

Vocabulaire 17.6 (Combinaison linéaire)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,\dots,x_n)\in E^n$. On appelle* combinaison linéaire *de $x_1,\dots,x_n$ tout vecteur de E du type $\sum_{k=1}^n \lambda_k x_k$, où $(\lambda_1,\dots,\lambda_n)\in\mathbb{K}^n$. De même, pour $A\subset E$, on appelle* combinaison linéaire *(finie) d'éléments de A toute combinaison linéaire d'un nombre fini d'éléments de A.*

II Sous-espaces vectoriels

II.1 Généralités

Définition 17.7 (Sous-espace vectoriel)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $F\subset E$. F est dit* sous-espace vectoriel *de E lorsque F est un espace vectoriel muni des lois induites par celles de E.*

Proposition 17.8. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $F\subset E$. F est un sous-espace vectoriel de E* ssi *$F\neq\varnothing$ et $\forall(\lambda,\mu)\in\mathbb{K}^2$, $\forall(x,y)\in E^2$, $\lambda x+\mu y\in F$.*

Vocabulaire 17.9 (Vecteurs colinéaires)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(u,v)\in E^2$. u et v sont dits* colinéaires *lorsque $u=0_E$* ou *$\exists\lambda\in\mathbb{K}$, $v=\lambda u$.*

Définition 17.10 (Droite et plan)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(u,v)\in(E\backslash\{0_E\})^2$, avec u et v non colinéaires. On appelle* droite dirigée par *u le sous-espace vectoriel $\mathcal{D}_u = \{\lambda u,\ \lambda\in\mathbb{K}\}$; on appelle* plan dirigé par *u* et *v le sous-espace vectoriel $\{\lambda u+\mu v,\ (\lambda,\mu)\in\mathbb{K}^2\}$.*

II.2 Opérations ensemblistes et espaces vectoriels

Proposition 17.11. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(F_i)_{i\in I}$ une famille de sous-espaces vectoriels de E, où I est un ensemble quelconque. Alors $\bigcap_{i\in I} F_i$ est un sous-espace vectoriel de E.*

Définition 17.12 (Espace vectoriel engendré par une partie)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $A\subset E$. On appelle* espace vectoriel engendré par *A, noté* $\mathrm{Vect}(A)$*, le plus petit sous-espace vectoriel de E contenant A.*

Lemme 17.13. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. F un sous-espace vectoriel de E. Alors toute combinaison linéaire d'éléments de F est dans F.*

Proposition 17.14. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $A\subset E$, $A\neq\varnothing$. Alors* $\mathrm{Vect}(A)$ *est l'ensemble des combinaisons linéaires d'éléments de A.*

II.3 Somme de sous-espaces vectoriels

Notation 17.15. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $F_1,\dots,F_n$ n sous-espaces vectoriels de E. On note*

$$\sum_{i=1}^{n} F_i = \left\{ \sum_{i=1}^{n} f_i,\ (f_1,\dots,f_n) \in \prod_{i=1}^{n} F_i \right\}.$$

Proposition 17.16. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $F_1,\dots,F_n$ n sous-espaces vectoriels de E.*

$$\mathrm{Vect}\left(\bigcup_{i=1}^{n} F_i\right) = \sum_{i=1}^{n} F_i.$$

II.4 Somme directe de deux sous-espaces vectoriels

Définition 17.17 (Somme directe)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. F_1,F_2 deux sous-espaces vectoriels de E. On dit que la somme F_1+F_2 est* directe*, et on la note alors $F_1 \oplus F_2$, lorsque $\forall x \in (F_1+F_2),\ \exists!(f_1,f_2) \in F_1 \times F_2,\ x = f_1+f_2$.*

Proposition 17.18. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. F_1,F_2 deux sous-espaces vectoriels de E.*

$$F_1+F_2 \text{ est directe} \iff \forall (f_1,f_2) \in F_1 \times F_2,\ 0_E = f_1+f_2 \Rightarrow f_1 = f_2 = 0_E \quad \text{(i)}$$
$$\iff F_1 \cap F_2 = \{0_E\}. \quad \text{(ii)}$$

Définition 17.19 (Sous-espaces vectoriels supplémentaires)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. F_1,F_2 deux sous-espaces vectoriels de E. On dit que F_1 et F_2 sont* supplémentaires *lorsque $F_1 \oplus F_2 = E$.*

Proposition 17.20. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. F_1,F_2 deux sous-espaces vectoriels de E. F_1 et F_2 sont supplémentaires* ssi *$F_1+F_2 = E$ et $F_1 \cap F_2 = \{0_E\}$.*

Proposition 17.21. *On note $\mathcal{P} = \left\{ f \in \mathbb{R}^{\mathbb{R}},\ f \text{ paire} \right\}$, $\mathcal{I} = \left\{ f \in \mathbb{R}^{\mathbb{R}},\ f \text{ impaire} \right\}$.*

$$\mathbb{R}^{\mathbb{R}} = \mathcal{P} \oplus \mathcal{I}.$$

II.5 Somme directe de n sous-espaces vectoriels

Définition 17.22 (Somme directe)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $F_1,\dots,F_n$ n sous-espaces vectoriels de E. On dit que la somme $\sum_{i=1}^{n} F_i$ est* directe *lorsque*

$$\forall x \in \sum_{i=1}^{n} F_i,\ \exists!(f_1,\dots,f_n) \in \prod_{i=1}^{n} F_i,\ x = \sum_{i=1}^{n} f_i.$$

On note alors cette somme

$$\bigoplus_{i=1}^{n} F_i.$$

Proposition 17.23. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $F_1,\dots,F_n$ n sous-espaces vectoriels de E.*

$$\sum_{i=1}^{n} F_i \text{ est directe}$$
$$\iff \forall (f_1,\dots,f_n) \in \prod_{i=1}^{n} F_i,\ 0_E = \sum_{i=1}^{n} f_i \Rightarrow \forall i \in [\![1,n]\!],\ f_i = 0_E.$$

Proposition 17.24. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $F_1,\dots,F_n$ n sous-espaces vectoriels de E. Si $\sum_{i=1}^n F_i$ est directe, alors $\forall (i,j)\in[\![1,p]\!]^2,\ i\neq j \Longrightarrow F_i\cap F_j=\{0_E\}$.*

Proposition 17.25. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $F_1,\dots,F_n$ n sous-espaces vectoriels de E. Si $E=\bigoplus_{i=1}^n F_i$, alors pour tout $j\in[\![1,n]\!]$, un supplémentaire de F_j est*

$$\bigoplus_{\substack{1\leqslant i\leqslant n\\ i\neq j}} F_i.$$

III Familles libres, génératrices et bases

III.1 Systèmes finis de vecteurs

Vocabulaire 17.26 (Système fini de vecteurs)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. On appelle* système fini de vecteurs *toute suite $(x_1,\dots,x_n)\in E^n$.*

Définition 17.27 (Système libre ou lié)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,\dots,x_n)$ un système de n vecteurs de E. On dit que le système $(x_1,\dots,x_n)$ est* libre *lorsque*

$$\forall(\lambda_1,\dots,\lambda_n)\in\mathbb{K}^n,\ \sum_{i=1}^n \lambda_i x_i=0_E \Longrightarrow \forall i\in[\![1,n]\!],\ \lambda_i=0_{\mathbb{K}}.$$

On dit que le système $(x_1,\dots,x_n)$ est lié *s'il n'est pas libre.*

Proposition 17.28. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,x_2)\in E^2$. Le système (x_1,x_2) est lié* ssi *x_1 et x_2 sont colinéaires, i.e. $x_2=0_E$* ou *$\exists\lambda\in\mathbb{K},\ x_1=\lambda x_2$.*

Proposition 17.29. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,\dots,x_n)\in E^n$.*

(i) *$(x_1,\dots,x_n)$ lié* ssi *$\exists(\lambda_1,\dots,\lambda_n)\in\mathbb{K}^n\backslash\{(0_{\mathbb{K}},\dots,0_{\mathbb{K}})\},\ \sum_{i=1}^n\lambda_i x_i=0_E$.*

(ii) *Un système contenant un vecteur nul est lié.*

(iii) *Un système contenant deux vecteurs colinéaires est lié.*

(iv) *Un système est lié* ssi *un des vecteurs est CL des autres.*

Proposition 17.30. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,\dots,x_n)\in E^n$. $(x_1,\dots,x_n)$ est libre* ssi *tout vecteur de E s'écrit d'au plus une façon comme combinaison linéaire de $x_1,\dots,x_n$.*

Proposition 17.31. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,\dots,x_n)\in E^n$ libre. $x\in E$. Alors $(x_1,\dots,x_n,x)$ est lié* ssi *$x\in\mathrm{Vect}(x_1,\dots,x_n)$.*

Vocabulaire 17.32 (Sur-système et sous-système)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,\dots,x_n)\in E^n$. On appelle* sur-système *de $(x_1,\dots,x_n)$ tout système contenant $(x_1,\dots,x_n)$. On appelle* sous-système *de $(x_1,\dots,x_n)$ tout système dont $(x_1,\dots,x_n)$ est sur-système.*

Proposition 17.33.

(i) *Tout sous-système d'un système libre est libre.*

(ii) *Tout sur-système d'un système lié est lié.*

III.2 Systèmes générateurs

Définition 17.34 (Famille génératrice)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. On dit que $(x_1,\dots,x_n)\in E^n$ est une* famille génératrice *(ou* système générateur*) de E lorsque $E=\mathrm{Vect}(x_1,\dots,x_n)$.*

Proposition 17.35. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. Tout sur-système d'un système générateur de E génère E.*

Proposition 17.36. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,\dots,x_n)\in E^n$ un système générateur de E. $\mathcal{H}$ un système de vecteurs de E.*

$$\mathcal{H} \text{ génère } E \iff \forall i\in[\![1,n]\!],\ x_i\in\mathrm{Vect}(\mathcal{H}).$$

III.3 Base d'un espace vectoriel

Définition 17.37 (Base)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,\dots,x_n)\in E^n$. $(x_1,\dots,x_n)$ est dit* base *de E lorsque $(x_1,\dots,x_n)$ génère E et $(x_1,\dots,x_n)$ est libre.*

Proposition 17.38. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_1,\dots,x_n)\in E^n$. $(x_1,\dots,x_n)$ est une base de E* ssi

$$\forall x\in E,\ \exists!(\lambda_1,\dots,\lambda_n)\in\mathbb{K}^n,\ x=\sum_{k=1}^{n}\lambda_k x_k.$$

On dit alors que $(\lambda_1,\dots,\lambda_n)$ sont les composantes *ou* coordonnées *de x dans la base $(x_1,\dots,x_n)$.*

III.4 Famille quelconque de vecteurs

Définition 17.39 (Famille presque nulle)**.** *$(\lambda_i)_{i\in I}$ une famille d'éléments de $\mathbb{K}$, où I est un ensemble quelconque non vide. On dit que la famille $(\lambda_i)_{i\in I}$ est* presque nulle *lorsque tous les λ_i sont nuls excepté un nombre fini d'entre eux.*

Définition 17.40 (Combinaison linéaire)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_i)_{i\in I}$ une famille de vecteurs de E. $x\in E$. On dit que x est* combinaison linéaire *de la famille $(x_i)_{i\in I}$ lorsqu'il existe une famille presque nulle $(\lambda_i)_{i\in I}$ de scalaires t.q. $x=\sum_{i\in I}\lambda_i x_i$.*

Définition 17.41 (Famille génératrice)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_i)_{i\in I}$ une famille de vecteurs de E. On dit que $(x_i)_{i\in I}$ est une* famille génératrice *de E lorsque tout vecteur de E est CL des $(x_i)_{i\in I}$. Autrement dit, $E=\mathrm{Vect}\left((x_i)_{i\in I}\right)$.*

Définition 17.42 (Famille libre)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_i)_{i\in I}$ une famille de vecteurs de E. On dit que $(x_i)_{i\in I}$ est* libre *dans E lorsque pour toute famille presque nulle $(\lambda_i)_{i\in I}$ de scalaires*

$$\sum_{i\in I}\lambda_i x_i=0_E \Longrightarrow \forall i\in I,\ \lambda_i=0_{\mathbb{K}}.$$

Proposition 17.43. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(x_i)_{i\in\mathbb{N}}$ une famille de vecteurs de E. $(x_i)_{i\in\mathbb{N}}$ est libre* ssi *pour tout $n\in\mathbb{N}$, $(x_0,\dots,x_n)$ est libre.*

Vocabulaire 17.44 (Dimension finie ou infinie)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. On dit que E est de* dimension finie *si E admet une famille génératrice finie. Sinon, on dit que E est de* dimension infinie*.*

Remarque 17.45. *Les propositions 17.29, 17.30, 17.31, 17.33, 17.35 et 17.36 restent valables en remplaçant système fini de vecteurs par famille de vecteurs.*

IV Applications linéaires

IV.1 Généralités

Définition 17.46 (Application linéaire)**.** *$(E,+,\cdot)$ et $(F,+,\cdot)$ deux $\mathbb{K}$-espaces vectoriels. $u : E \to F$ une application. On dit que u est une* application linéaire *lorsque*

(i) $\forall (x,y) \in E^2,\ u(x+y) = u(x) + u(y)$,

(ii) $\forall \lambda \in \mathbb{K},\ \forall x \in E,\ u(\lambda \cdot x) = \lambda \cdot u(x)$.

Proposition 17.47. *$u : E \to F$ une application linéaire. Alors $u(0_E) = 0_F$.*

Proposition 17.48. *$(E,+,\cdot)$ et $(F,+,\cdot)$ deux $\mathbb{K}$-espaces vectoriels. $u : E \to F$ une application. u est une application linéaire* ssi

$$\forall (x,y) \in E^2,\ \forall (\lambda,\mu) \in \mathbb{K}^2,\ u(\lambda x + \mu y) = \lambda u(x) + \mu u(y).$$

Proposition 17.49. *$u : E \to F$ une application linéaire. Si E admet une famille génératrice $(e_i)_{i\in I}$, alors u est entièrement déterminée par $(u(e_i))_{i\in I}$.*

IV.2 Image et noyau

Définition 17.50 (Image et noyau)**.** *$u : E \to F$ une application linéaire. On définit :*

$$\operatorname{Im} u = u(E) \qquad \text{et} \qquad \operatorname{Ker} u = u^{-1}\left(\{0_F\}\right).$$

Lemme 17.51. *$u : E \to F$ une application linéaire. G et H des sous-espaces vectoriels de respectivement E et F. Alors $u(G)$ est un sous-espace vectoriel de F et $u^{-1}(H)$ est un sous-espace vectoriel de E.*

Proposition 17.52. *$u : E \to F$ une application linéaire. Alors $\operatorname{Ker} u$ est un sous-espace vectoriel de E et $\operatorname{Im} u$ est un sous-espace vectoriel de F.*

Proposition 17.53. *$u : E \to F$ une application linéaire. Si E admet une famille génératrice $(e_i)_{i\in I}$, alors*

$$\operatorname{Im} u = \operatorname{Vect}\left(u(e_i)_{i\in I}\right).$$

Proposition 17.54. *$u : E \to F$ une application linéaire. $\lambda \in \mathbb{K}^*$. Alors l'application λu est linéaire, et on a*

$$\operatorname{Ker}(\lambda u) = \operatorname{Ker} u \qquad \text{et} \qquad \operatorname{Im}(\lambda u) = \operatorname{Im} u.$$

Proposition 17.55. *$u : E \to F$ une application linéaire.*

$$u \text{ injective} \iff \operatorname{Ker} u = \{0_E\}, \tag{i}$$

$$u \text{ surjective} \iff \operatorname{Im} u = F. \tag{ii}$$

Vocabulaire 17.56. *$u : E \to F$ une application linéaire.*

(i) *u est dit* isomorphisme *si u est bijective.*

(ii) *u est dit* endomorphisme *si $E = F$.*

(iii) *u est dit* automorphisme *si u est un endomorphisme bijectif.*

Proposition 17.57. *$u : E \to F$ un isomorphisme. Alors u^{-1} est aussi un isomorphisme.*

IV.3 Restrictions

Proposition 17.58. *$u : E \to F$ une application linéaire. G un sous-espace vectoriel de E. Alors l'application $u_{|G}$ est linéaire et*

$$\operatorname{Ker} u_{|G} = G \cap \operatorname{Ker} u.$$

Corollaire 17.59. *$u : E \to F$ une application linéaire. G un sous-espace vectoriel de E. Si u est injective, alors $u_{|G}$ est injective.*

IV.4 Opérations et applications linéaires

Notation 17.60. *$(E, +, \cdot)$ et $(F, +, \cdot)$ deux $\mathbb{K}$-espaces vectoriels. $\mathcal{L}(E, F)$ désigne l'ensemble des applications linéaires de E dans F. On note de plus $\mathcal{L}(E) = \mathcal{L}(E, E)$.*

Proposition 17.61. *$(E, +, \cdot)$ et $(F, +, \cdot)$ deux $\mathbb{K}$-espaces vectoriels. $(\mathcal{L}(E, F), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.*

Proposition 17.62. *$u : E \to F$ et $v : F \to G$ deux applications linéaires. Alors $v \circ u$ est une application linéaire.*

Proposition 17.63. *$u : E \to F$ et $v : F \to G$ deux applications linéaires.*

$$\operatorname{Im} u \subset \operatorname{Ker} v \iff v \circ u = 0.$$

IV.5 Résolution d'équations linéaires

Proposition 17.64. *$u : E \to F$ une application linéaire, $b \in F$. L'équation $u(x) = b$ est dite* linéaire *et a pour solution $\varnothing$ si $b \notin \operatorname{Im} u$, ou bien $\{x_0 + x,\ x \in \operatorname{Ker} u\}$, où x_0 vérifie $u(x_0) = b$, si $b \in \operatorname{Im} u$. x_0 est dit* solution particulière *de l'équation.*

IV.6 Image d'une famille par une application linéaire

Proposition 17.65. *$u : E \to F$ une application linéaire.*

(i) *L'image d'une famille liée par u est liée.*

(ii) *L'image d'une famille génératrice de E par u génère $\operatorname{Im} u$.*

(iii) *Si u injective, alors l'image d'une famille libre par u est libre.*

(iv) *Si u surjective, alors l'image d'une famille génératrice de E par u génère F.*

(v) *Si u isomorphisme, alors l"image d'une base de E par u est une base de F.*

V Structure d'algèbre de $\mathcal{L}(E)$

Proposition 17.66. *$(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel. Alors $(\mathcal{L}(E), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel et $(\mathcal{L}(E), +, \circ)$ est un anneau. On dit que $\mathcal{L}(E)$ est une* algèbre.

Notation 17.67 (Groupe linéaire)**.** *On note $GL(E)$, dit* groupe linéaire *de E, l'ensemble des automorphismes de E.*

Proposition 17.68. *$(GL(E), \circ)$ est un groupe.*

Notation 17.69. *$u \in \mathcal{L}(E)$, $n \in \mathbb{N}$. On note $u^n = \underbrace{u \circ \cdots \circ u}_{n \text{ fois}}$ si $n \in \mathbb{N}^*$, $u^0 = id_E$. Si $u \in GL(E)$, $n \in \mathbb{Z}$, on note $u^n = \left(u^{-1}\right)^{-n}$ pour $n < 0$.*

Vocabulaire 17.70 (Nilpotence et idempotence)**.** $u \in \mathcal{L}(E)$.

(i) *u est dit* nilpotent *lorsque* $\exists n \in \mathbb{N},\ u^n = 0$. *L'entier* $\min\{n \in \mathbb{N},\ u^n = 0\}$ *est alors dit* indice *de u.*

(ii) *u est dit* idempotent *lorsque* $u^2 = u$.

Proposition 17.71. *$u \in \mathcal{L}(E)$ nilpotent d'indice n.*

(i) *u non injective.*

(ii) $(id_E - u) \in GL(E)$.

(iii) $\exists x_0 \in E,\ \left(u^k(x_0)\right)_{k\in[\![0,n[\![}$ *est libre dans E.*

Démonstration. (ii) Montrer que $(id_E - u)\sum_{k=0}^{n-1} u^k = id_E$. (iii) Choisir $x_0 \in E$ t.q. $u^{n-1}(x_0) \neq 0$ et montrer que x_0 convient. □

VI Projecteurs et symétries

Définition 17.72 (Projecteur)**.** $p \in \mathcal{L}(E)$ *est dit* projecteur *de E lorsque* $p^2 = p$.

Définition 17.73 (Symétrie)**.** $s \in \mathcal{L}(E)$ *est dit* symétrie *de E lorsque* $s^2 = id_E$.

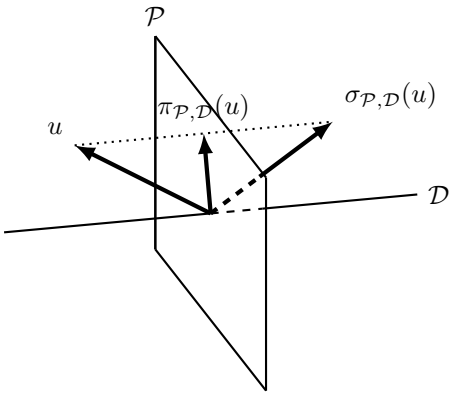
Proposition 17.74. *$s \in \mathcal{L}(E)$. s est une symétrie de E* ssi $\frac{s+id_E}{2}$ *est un projecteur de E.*

Définition 17.75 (Projection et symétrie)**.** $(E, +, \cdot)$ *un $\mathbb{K}$-espace vectoriel. F et G deux sous-espaces vectoriels de E t.q. $F \oplus G = E$. On a alors* $\forall x \in E,\ \exists!(x_F, x_G) \in F \times G,\ x = x_F + x_G$. *On appelle* projection *sur F parallèlement à G l'application*

$$\pi_{F,G} : \left| \begin{array}{l} E \longrightarrow E \\ x \longmapsto x_F \end{array} \right. .$$

On appelle symétrie *de base F parallèlement à G l'application*

$$\sigma_{F,G} : \left| \begin{array}{l} E \longrightarrow E \\ x \longmapsto x_F - x_G \end{array} \right. .$$



Projection et symétrie sur un plan dans $\mathbb{R}^3$

Remarque 17.76. *Pour $u \in \mathcal{L}(E)$,* $\mathrm{Ker}(u - id_E)$ *est l'*ensemble des vecteurs invariants par u.

Proposition 17.77. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. F et G deux sous-espaces vectoriels de E t.q. $F \oplus G = E$.*

(i) *$\pi_{F,G}$ est un projecteur.*

(ii) *$\sigma_{F,G}$ est une symétrie.*

(iii) $\operatorname{Im} \pi_{F,G} = \operatorname{Ker}(\pi_{F,G} - id_E) = F$ *et* $\operatorname{Ker} \pi_{F,G} = G$.

(iv) $\operatorname{Ker}(\sigma_{F,G} - id_E) = F$ *et* $\operatorname{Ker}(\sigma_{F,G} + id_E) = G$.

(v) $\pi_{G,F} = id_E - \pi_{F,G}$ *et* $\pi_{G,F} \circ \pi_{F,G} = 0$.

Proposition 17.78.

(i) *$p \in \mathcal{L}(E)$ un projecteur. Alors* $\operatorname{Im} p \oplus \operatorname{Ker} p = E$ *et* $p = \pi_{\operatorname{Im} p, \operatorname{Ker} p}$.

(ii) *$s \in \mathcal{L}(E)$ une symétrie. Alors* $\operatorname{Ker}(s - id_E) \oplus \operatorname{Ker}(s + id_E) = E$ *et* $s = \sigma_{\operatorname{Ker}(s-id_E), \operatorname{Ker}(s+id_E)}$.

Définition 17.79 (Projections associées à une somme directe)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(F_1, \dots, F_r)$ r sous-espaces vectoriels de E t.q. $E = \bigoplus_{i=1}^r F_i$. On appelle* projections associées à cette somme directe *les projections $p_1, \dots, p_r$, où p_j est la projection sur F_j parallèlement à $\bigoplus_{\substack{1 \leqslant i \leqslant r \\ i \neq j}} F_i$, pour $j \in [\![1, r]\!]$.*

Proposition 17.80. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(F_1, \dots, F_r)$ r sous-espaces vectoriels de E t.q. $E = \bigoplus_{i=1}^r F_i$. $p_1, \dots, p_r$ les projections associées à cette somme directe. Alors*

$$\forall (i,j) \in [\![1,r]\!]^2,\ i \neq j \Longrightarrow p_i \circ p_j = 0 \qquad \text{et} \qquad \sum_{i=1}^r p_i = id_E.$$

Proposition 17.81. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. $(F_1, \dots, F_r)$ r sous-espaces vectoriels de E t.q. $E = \bigoplus_{i=1}^r F_i$. $u \in \mathcal{L}(E,F)$. Alors u est entièrement déterminée par ses restrictions à chacun des F_i. On pose de plus, pour $i \in [\![1,r]\!]$,*

$$\hat{p}_i : \left| \begin{array}{l} E \longrightarrow F_i \\ x \longmapsto p_i(x) \end{array} \right. ,$$

où $p_1, \dots, p_r$ sont les projections associées à la somme directe $E = \bigoplus_{i=1}^r F_i$. Alors

$$u = \sum_{i=1}^r u_{|F_i} \circ \hat{p}_i.$$

VII Noyaux, formes linéaires et hyperplans

VII.1 Définitions

Définition 17.82 (Forme linéaire)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. On appelle* forme linéaire *toute application linéaire de E dans $\mathbb{K}$. On note $E^* = \mathcal{L}(E, \mathbb{K})$, dit* espace dual *de E.*

Définition 17.83 (Hyperplan)**.** *On appelle* hyperplan *tout noyau d'une forme linéaire non nulle.*

Proposition 17.84. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. Tout hyperplan de E est un sous-espace vectoriel de E.*

VII.2 Caractérisation des hyperplans

Proposition 17.85. $(E, +, \cdot)$ *un* $\mathbb{K}$*-espace vectoriel.* $H \subset E$*.* H *est un hyperplan de* E ssi H *admet comme supplémentaire une droite vectorielle de* E*. Dans ce cas, on a*

$$\forall a \in E \backslash H,\ E = H \oplus \mathrm{Vect}(a).$$

Démonstration. ($\Rightarrow$) Choisir $a \in E\backslash H$ et montrer que $E = H \oplus \mathrm{Vect}(a)$. ($\Leftarrow$) Supposer que $E = H \oplus \mathrm{Vect}(a)$, où $a \in E\backslash\{0\}$ et définir l'application $\varphi : x \in E \longmapsto$ l'unique scalaire λ t.q. $(x - \lambda a) \in H$. Montrer que φ est une forme linéaire et que $H = \mathrm{Ker}\,\varphi$. □

VII.3 Formes linéaires colinéaires

Proposition 17.86. *Deux formes linéaires non nulles sont colinéaires* ssi *elles ont le même noyau.*

Démonstration. ($\Leftarrow$) Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel, $(\varphi, \psi) \in (E^*\backslash\{0\})^2$ t.q. $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\psi$. Comme $\mathrm{Ker}\,\varphi$ est un hyperplan, on a (par la proposition 17.85) : $\exists a \in E\backslash\{0\}$, $E = \mathrm{Ker}\,\varphi \oplus \mathrm{Vect}(a)$. Montrer alors que φ et ψ sont colinéaires sur $\mathrm{Ker}\,\varphi$ et sur $\mathrm{Vect}(a)$. □

Chapitre 18

Espaces Vectoriels de Dimension Finie

Vocabulaire 18.1 (Dimension finie ou infinie)**.** $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel. On dit que* E *est de* dimension finie *si* E *admet une famille génératrice finie. Sinon, on dit que* E *est de* dimension infinie*.*

I Théorème de la base incomplète

Théorème 18.2 (Théorème de la base incomplète)**.** $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie,* $E \neq \{0\}$*.* $\mathfrak{L}$ *une famille libre finie de* E *(éventuellement* $\varnothing$*).* $\mathcal{G}$ *une famille génératrice finie de* E*. Alors il existe une base de* E *obtenue en complétant la famille* $\mathfrak{L}$ *avec uniquement des vecteurs de* $\mathcal{G}$*.*

Démonstration. Considérer $A = \{\text{card}(\mathfrak{L}\cup\mathcal{C}),\ \mathcal{C}\subset\mathcal{G},\ \mathfrak{L}\cup\mathcal{C} \text{ libre}\}$. On a $A\subset\mathbb{N}$, $A\neq\varnothing$ et A majoré par $\text{card}\,\mathfrak{L}+\text{card}\,\mathcal{G}$, donc A admet un plus grand élément noté $\text{card}(\mathfrak{L}\cup\mathcal{C}_0)$. Montrer alors que $\mathfrak{L}\cup\mathcal{C}_0$ est une base de E. Soit $x\in\mathcal{G}$. Supposer $x\notin\mathfrak{L}\cup\mathcal{C}_0$, sinon il est évident que $x\in\text{Vect}(\mathfrak{L}\cup\mathcal{C}_0)$. Par maximalité de $\text{card}(\mathfrak{L}\cup\mathcal{C}_0)$, la famille $\mathfrak{L}\cup\mathcal{C}_0\cup\{x\}$ est liée (puisque $\mathcal{C}_0\cup\{x\}\subset\mathcal{G}$) ; et $\mathfrak{L}\cup\mathcal{C}_0$ est libre, donc $x\in\text{Vect}(\mathfrak{L}\cup\mathcal{C}_0)$, d'où $\mathcal{G}\subset\text{Vect}(\mathfrak{L}\cup\mathcal{C}_0)$. Ainsi $E=\text{Vect}(\mathcal{G})\subset\text{Vect}(\mathfrak{L}\cup\mathcal{C}_0)$, donc $E=\text{Vect}(\mathfrak{L}\cup\mathcal{C}_0)$. Et $\mathfrak{L}\cup\mathcal{C}_0$ est libre, donc $\mathfrak{L}\cup\mathcal{C}_0$ est une base de E. □

Corollaire 18.3. *Tout espace vectoriel de dimension finie admet une base.*

II Dimension d'un espace vectoriel de dimension finie

Lemme 18.4 (Lemme de Steinitz)**.** $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel,* $n\in\mathbb{N}$*. Alors* $(n+1)$ *vecteurs d'un sous-espace vectoriel de* E *généré par* n *vecteurs sont liés.*

Démonstration. Récurrence. $\mathcal{P}(n):\forall(a_1,\dots,a_n)\in E^n,\forall(x_1,\dots,x_{n+1})\in(\text{Vect}(a_1,\dots,a_n))^{n+1}$, $(x_1,\dots,x_{n+1})$ liée. $\mathcal{P}(0)$ vraie. Fixer $n\in\mathbb{N}$ t.q. $\mathcal{P}(n)$ vraie. Soit $(a_1,\dots,a_{n+1})\in E^{n+1}$, $F=\text{Vect}(a_1,\dots,a_{n+1})$, $(x_1,\dots,x_{n+2})\in F^{n+2}$. On peut supposer qu'un des vecteurs $x_1,\dots,x_{n+2}$, qu'on note x_{n+2}, n'appartient pas à $\text{Vect}(a_1,\dots,a_n)$ (sinon, par $\mathcal{P}(n)$, $(x_1,\dots,x_{n+2})$ est liée). On a $F=\text{Vect}(a_1,\dots,a_n)\oplus\text{Vect}(a_{n+1})$. Poser alors $p\in\mathfrak{L}(F)$ la projection sur $\text{Vect}(a_{n+1})$ parallèlement à $\text{Vect}(a_1,\dots,a_n)$, et $q=id_F-p$. Écrire $x_{n+2}=p(x_{n+2})+q(x_{n+2})$, avec $p(x_{n+2})\neq 0$ car $x_{n+2}\notin\text{Vect}(a_1,\dots,a_n)$, donc $p(x_{n+2})=\lambda_{n+2}a_{n+1}$, où $\lambda_{n+2}\in\mathbb{K}^*$. Pour $i\in[\![1,n+1]\!]$, $x_i=p(x_i)+q(x_i)=\lambda_i a_{n+1}+q(x_i)$, où $\lambda_i\in\mathbb{K}$, donc $y_i=\lambda_i x_{n+2}-\lambda_{n+2}x_i\in\text{Vect}(a_1,\dots,a_n)$. Par $\mathcal{P}(n)$, $(y_1,\dots,y_{n+1})$ liée. Donc

il existe $(\alpha_1, \dots, \alpha_{n+1}) \in \mathbb{K}^{n+1}$, avec $\alpha_{i_0} \neq 0$, t.q. $\sum_{i=1}^{n+1} \alpha_i y_i = \left(\sum_{i=1}^{n+1} \alpha_i \lambda_i\right) x_{n+2} - \lambda_{n+2} \left(\sum_{i=1}^{n+1} \alpha_i x_i\right) = 0$. Comme $\lambda_{n+2} \neq 0$ et $\alpha_{i_0} \neq 0$, le coefficient de x_{i_0} est non nul, donc $(x_1, \dots, x_{n+2})$ est liée. Donc $\mathcal{P}(n+1)$ vraie. □

Corollaire 18.5. *Toute sur-famille d'une famille génératrice d'un espace vectoriel est liée.*

Théorème 18.6. $(E, +, \cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* $\mathfrak{L}$ *une famille libre finie de* E*.* $\mathcal{G}$ *une famille génératrice finie de* E*.*

$$\operatorname{card} \mathfrak{L} \leqslant \operatorname{card} \mathcal{G}.$$

Corollaire 18.7. $(E, +, \cdot)$ *un* $\mathbb{K}$*-espace vectoriel.* E *est de dimension infinie* ssi *pour tout* $n \in \mathbb{N}$*, il existe une famille libre de* E *de* n *éléments.*

Démonstration. ($\Rightarrow$) Par récurrence. ($\Leftarrow$) Par l'absurde. □

Définition 18.8 (Dimension)**.** $(E, +, \cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie. Alors toutes les bases de* E *ont le même nombre d'éléments, noté* $\dim E$*.*

Démonstration. Utiliser le théorème 18.6. □

Proposition 18.9. $(E, +, \cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* $\mathcal{B}$ *une famille de* E*.*

$$\begin{aligned} \mathcal{B} \text{ est une base de } E &\iff \mathcal{B} \text{ est libre et } \mathcal{B} \text{ génère } E && \text{(i)} \\ &\iff \mathcal{B} \text{ est libre et } \operatorname{card} \mathcal{B} = \dim E && \text{(ii)} \\ &\iff \mathcal{B} \text{ génère } E \text{ et } \operatorname{card} \mathcal{B} = \dim E. && \text{(iii)} \end{aligned}$$

Proposition 18.10. $(E, +, \cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* F *un sous-espace vectoriel de* E*. Alors* F *est de dimension finie et* $\dim F \leqslant \dim E$*, avec égalité* ssi $F = E$*.*

Démonstration. Noter $\mathfrak{H}$ l'ensemble des familles libres de F puis considérer l'ensemble $A = \{\operatorname{card} \mathfrak{L},\ \mathfrak{L} \in \mathfrak{H}\}$. Poser $\mathfrak{L}_0 \in \mathfrak{H}$ t.q. $\operatorname{card} \mathfrak{L}_0 = \max A$, et montrer que $\mathfrak{L}_0$ est une base de F, avec $\operatorname{card} \mathfrak{L}_0 \leqslant \dim E$. □

III Somme de sous-espaces vectoriels d'un espace vectoriel de dimension finie

III.1 Somme de deux sous-espaces vectoriels

Proposition 18.11. $(E, +, \cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* F *un sous-espace vectoriel de* E*. Alors* F *admet un supplémentaire dans* E*. De plus, tout supplémentaire de* F *est de dimension égale à* $(\dim E - \dim F)$*.*

Démonstration. Choisir une base b de F et utiliser le théorème de la base incomplète (théorème 18.2) pour obtenir une base $\mathcal{B} \supset b$ de E, puis montrer que $E = F \oplus \operatorname{Vect}(\mathcal{B} \backslash b)$. □

Proposition 18.12. $(E, +, \cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* F, G *deux sous-espaces vectoriels de* E*.*

(i) $\dim(F + G) = \dim F + \dim G - \dim(F \cap G)$.

(ii) $\dim(F+G) \leqslant \dim F + \dim G$, *avec égalité* ssi *la somme* $F+G$ *est directe.*

Démonstration. (i) Montrer que $F+G = F \oplus H$, où H est un supplémentaire de $F \cap G$ dans G. Utiliser ensuite la proposition 18.11. □

Proposition 18.13. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* F, G *deux sous-espaces vectoriels de* E*. La somme* $F+G$ *est directe* ssi *il existe une base de* $F+G$ *réunion disjointe d'une base de* F *et d'une base de* G*. De plus, dans ce cas, toute réunion d'une base de* F *et d'une base de* G *est une base de* $F \oplus G$*.*

Vocabulaire 18.14 (Base adaptée)**.** $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* F, G *deux sous-espaces vectoriels de* E *en somme directe. On appelle* base adaptée *à* $F \oplus G$ *toute réunion d'une base de* F *et d'une base de* G*.*

III.2 Supplémentaires

Notation 18.15. *Si* A *et* B *sont deux ensembles disjoints (i.e.* $A \cap B = \varnothing$*), on note leur union* $A \sqcup B$*.*

Proposition 18.16. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* F, G *deux sous-espaces vectoriels de* E*.*

$$E = F \oplus G \iff \exists \mathcal{B}_1 \text{ base de } F,\ \exists \mathcal{B}_2 \text{ base de } G,\ \mathcal{B}_1 \sqcup \mathcal{B}_2 \text{ base de } E \quad \text{(i)}$$

$$\iff \dim F + \dim G = \dim E \text{ et } F \cap G = \{0\} \quad \text{(ii)}$$

$$\iff \dim F + \dim G = \dim E \text{ et } F + G = E. \quad \text{(iii)}$$

Corollaire 18.17. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* H *un sous-espace vectoriel de* E*.* H *est un hyperplan de* E ssi $\dim H = \dim E - 1$*.*

III.3 Somme de n sous-espaces vectoriels

Proposition 18.18. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* $F_1, \dots, F_r$ r *sous-espaces vectoriels de* E*. Alors* $\dim\left(\sum_{i=1}^r F_i\right) \leqslant \sum_{i=1}^r \dim F_i$*, avec égalité* ssi $\sum_{i=1}^r F_i$ *est directe.*

Proposition 18.19. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* $F_1, \dots, F_r$ r *sous-espaces vectoriels de* E*.* $\sum_{i=1}^r F_i$ *est directe* ssi *il existe une base de* $\sum_{i=1}^r F_i$ *réunion disjointe de bases de* $F_1, \dots, F_r$*. Dans ce cas, toute réunion de bases de* $F_1, \dots, F_r$ *est une base de* $\bigoplus_{i=1}^r F_i$*.*

Proposition 18.20. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* $F_1, \dots, F_r$ r *sous-espaces vectoriels de* E*.*

$$E = \bigoplus_{i=1}^r F_i \iff \dim E = \sum_{i=1}^r \dim F_i = \dim\left(\sum_{i=1}^r F_i\right) \quad \text{(i)}$$

$$\iff \forall i \in [\![1,r]\!],\ \exists \mathcal{B}_i \text{ base de } F_i,\ \bigsqcup_{i=1}^r \mathcal{B}_i \text{ base de } E \quad \text{(ii)}$$

$$\iff \dim E = \sum_{i=1}^r \dim F_i \quad \text{(iii)}$$

et 0 *se décompose de manière unique sur* $\sum_{i=1}^r F_i$*.*

III.4 Espace produit

Proposition 18.21. *$(E,+,\cdot)$ et $(F,+,\cdot)$ deux $\mathbb{K}$-espaces vectoriels de dimension finie. $n \in \mathbb{N}^*$.*

(i) *$E \times F$ est un espace vectoriel de dimension finie et* $\dim(E \times F) = \dim E + \dim F$.

(ii) *E^n est un espace vectoriel de dimension finie et* $\dim E^n = n \dim E$.

IV Applications linéaires et dimension finie

IV.1 Généralités

Proposition 18.22. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel de dimension p. $(F,+,\cdot)$ un $\mathbb{K}$-espace vectoriel quelconque. $(e_1,\dots,e_p)$ une base de E.*

$$\forall (f_1,\dots,f_p) \in F^p,\ \exists! u \in \mathcal{L}(E,F),\ \forall i \in [\![1,p]\!],\ u(e_i) = f_i.$$

Proposition 18.23. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel de dimension finie. $(F,+,\cdot)$ un $\mathbb{K}$-espace vectoriel quelconque. $\mathcal{B}$ une base de E. $u \in \mathcal{L}(E,F)$.*

(i) *u est injective* ssi *$u(\mathcal{B})$ est libre dans F.*

(ii) *u est surjective* ssi *$u(\mathcal{B})$ génère F.*

(iii) *u est un isomorphisme* ssi *$u(\mathcal{B})$ est une base de F.*

Proposition 18.24. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel de dimension finie. $(F,+,\cdot)$ un $\mathbb{K}$-espace vectoriel quelconque. E et F sont isomorphes* ssi *F est de dimension finie* et $\dim F = \dim E$.

Proposition 18.25. *$(E,+,\cdot)$ et $(F,+,\cdot)$ deux $\mathbb{K}$-espaces vectoriels de dimension finie. Alors $\mathcal{L}(E,F)$ est de dimension finie est*

$$\dim \mathcal{L}(E,F) = \dim E \dim F.$$

Démonstration (Première méthode)**.** Soit $(e_1,\dots,e_m)$ une base de E, $(f_1,\dots,f_n)$ une base de F. Pour $(i,j) \in [\![1,m]\!] \times [\![1,n]\!]$, poser $u_{i,j} \in \mathcal{L}(E,F)$ définie par $u_{i,j}(e_i) = f_j$ et $\forall k \in [\![1,m]\!] \backslash \{i\}$, $u_{i,j}(e_k) = 0$. Montrer alors que $(u_{i,j})_{\substack{i \in [\![1,m]\!] \\ j \in [\![1,n]\!]}}$ est une base de $\mathcal{L}(E,F)$. □

Démonstration (Deuxième méthode)**.** Soit $(e_1,\dots,e_m)$ une base de E. Montrer que l'application

$$\theta : \left| \begin{array}{ccc} \mathcal{L}(E,F) & \longrightarrow & F^m \\ u & \longmapsto & (u(e_1),\dots,u(e_m)) \end{array} \right.$$

est un isomorphisme, puis utiliser la proposition 18.24 et la proposition 18.21. □

Vocabulaire 18.26 (Isomorphisme canonique)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel de dimension n. $(e_1,\dots,e_n)$ une base de E. Alors l'isomorphisme*

$$\varphi : \left| \begin{array}{ccc} \mathbb{K}^n & \longrightarrow & E \\ (x_1,\dots,x_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} x_i e_i \end{array} \right.$$

est dit isomorphisme canonique.

Proposition 18.27. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel de dimension finie, A un sous-espace vectoriel de E. Alors tous les supplémentaires de A sont isomorphes.*

IV.2 Rang de vecteurs et d'applications linéaires

Définition 18.28 (Rang)**.** *$(E,+,\cdot)$ et $(F,+,\cdot)$ deux $\mathbb{K}$-espaces vectoriels.*

(i) *$(x_1,\dots,x_q)\in E^q$. On définit* $\operatorname{rg}(x_1,\dots,x_q)=\dim\operatorname{Vect}(x_1,\dots,x_q)$.

(ii) *$u\in\mathcal{L}(E,F)$. Si* $\operatorname{Im}u$ *est de dimension finie, on dit que* $\operatorname{rg}u$ *est fini et on définit* $\operatorname{rg}u=\dim\operatorname{Im}u$.

Proposition 18.29. *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel de dimension finie. $(x_1,\dots,x_q)\in E^q$.*

(i) $\operatorname{rg}(x_1,\dots,x_q)\leqslant\min(q,\dim E)$.

(ii) $\operatorname{rg}(x_1,\dots,x_q)=q\iff(x_1,\dots,x_q)$ *libre dans E.*

(iii) $\operatorname{rg}(x_1,\dots,x_q)=\dim E\iff(x_1,\dots,x_q)$ *génère E.*

(iv) $\operatorname{rg}(x_1,\dots,x_q)=q=\dim E\iff(x_1,\dots,x_q)$ *est une base de E.*

Proposition 18.30. *$u\in\mathcal{L}(E,F)$.*

(i) *Si E ou F est de dimension finie, alors* $\operatorname{rg}u$ *est fini.*

(ii) $\operatorname{rg}u\leqslant\min(\dim E,\dim F)$.

(iii) *Si $\mathcal{B}$ est une base de E, alors* $\operatorname{rg}u=\dim\operatorname{Vect}(u(\mathcal{B}))$.

IV.3 Rang et composition

Proposition 18.31. *$(E,+,\cdot)$, $(F,+,\cdot)$ et $(G,+,\cdot)$ trois $\mathbb{K}$-espaces vectoriels de dimension finie. $u\in\mathcal{L}(E,F)$, $v\in\mathcal{L}(F,G)$.*

(i) $\operatorname{rg}(v\circ u)\leqslant\min(\operatorname{rg}v,\operatorname{rg}u)$.

(ii) *v injective* $\Longrightarrow\operatorname{rg}(v\circ u)=\operatorname{rg}u$.

(iii) *u surjective* $\Longrightarrow\operatorname{rg}(v\circ u)=\operatorname{rg}v$.

(iv) *La composition à droite ou à gauche par un isomorphisme ne modifie pas le rang.*

IV.4 Théorème du rang

Théorème 18.32 (Théorème du rang)**.** *$(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel de dimension finie. $(F,+,\cdot)$ un $\mathbb{K}$-espace vectoriel quelconque. $u\in\mathcal{L}(E,F)$.*

$$\dim E=\operatorname{rg}u+\dim\operatorname{Ker}u.$$

Démonstration. Comme $\operatorname{Ker}u$ est un sous-espace vectoriel de E, qui est de dimension finie, $\operatorname{Ker}u$ admet un supplémentaire $\mathcal{H}$ dans E : $E=\mathcal{H}\oplus\operatorname{Ker}u$. Montrer alors que

$$\theta:\left|\begin{array}{l}\mathcal{H}\longrightarrow\operatorname{Im}u\\ h\longmapsto u(h)\end{array}\right.$$

est un isomorphisme. En déduire que $\dim E=\dim\mathcal{H}+\dim\operatorname{Ker}u=\dim\operatorname{Im}u+\dim\operatorname{Ker}u$. □

V Applications linéaires entre deux espaces de même dimension

V.1 Généralités

Proposition 18.33. *$(E,+,\cdot)$ et $(F,+,\cdot)$ deux $\mathbb{K}$-espaces vectoriels de dimension finie. $u\in\mathcal{L}(E,F)$.*

$$\dim E=\dim F\Longrightarrow(u\text{ injective}\Leftrightarrow u\text{ surjective}\Leftrightarrow u\text{ isomorphisme}).$$

V.2 Endomorphismes

Définition 18.34 (Inverses à gauche et à droite)**.** *$u \in \mathcal{L}(E)$. On dit que u admet un* inverse à gauche *(resp.* à droite*) s'il existe $v \in \mathcal{L}(E)$ t.q. $v \circ u = id_E$ (resp. $u \circ v = id_E$).*

Proposition 18.35. *$(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel de dimension finie. $u \in \mathcal{L}(E)$.*

$$u \text{ isomorphisme} \iff u \text{ admet un inverse à gauche} \quad \text{(i)}$$
$$\iff u \text{ admet un inverse à droite.} \quad \text{(ii)}$$

Dans ce cas, les deux inverses de u sont égaux à u^{-1}.

VI Suites récurrentes linéaires et équations différentielles

VI.1 Suites récurrentes linéaires

Proposition 18.36. *$(a, b) \in \mathbb{K} \times \mathbb{K}^*$. On note*

$$E = \left\{(u_n) \in \mathbb{K}^n,\ \forall n \in \mathbb{N},\ u_{n+2} = au_{n+1} + bu_n\right\}.$$

Alors E est un espace vectoriel de dimension 2.

VI.2 Équations différentielles

Théorème 18.37 (Théorème de Cauchy-Lipschitz linéaire)**.** *I intervalle. $(a, b) \in \mathbb{R}^2$. On note*

$$\mathscr{S} = \left\{y \in \mathbb{R}^I \text{ deux fois dérivable, } y'' = ay' + by\right\}.$$

Alors on a

$$\forall (\alpha, \beta) \in \mathbb{R}^2,\ \forall x_0 \in I,\ \exists! y \in \mathscr{S},\ \begin{cases} y(x_0) = \alpha \\ y'(x_0) = \beta \end{cases}.$$

Corollaire 18.38. *Avec les notations du théorème précédent, $\mathscr{S}$ est un espace vectoriel de dimension 2.*

VII Dualité

VII.1 Généralités

Notation 18.39 (Espace dual et bidual)**.** *$(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel. On note $E^* = \mathcal{L}(E, \mathbb{K})$, dit* espace dual *de E, et $E^{**} = \mathcal{L}(E^*, \mathbb{K})$, dit* espace bidual *de E.*

Proposition 18.40. *$(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel. Alors l'application*

$$\theta : \left| \begin{array}{l} E \longrightarrow E^{**} \\ x \longmapsto \left| \begin{array}{l} E^* \longrightarrow \mathbb{K} \\ \ell \longmapsto \ell(x) \end{array} \right. \end{array} \right.$$

est linéaire et injective.

Démonstration. Montrer d'abord la linéarité. Supposer alors par l'absurde qu'il existe $x \in (\operatorname{Ker}\theta) \setminus \{0\}$. En admettant que $\operatorname{Vect}(x)$ admet un supplémentaire H dans E, poser $\varphi : \left| \begin{array}{l} E \longrightarrow \mathbb{K} \\ \lambda x + h \longmapsto \lambda \end{array} \right.$, où $\lambda \in \mathbb{K}$, $h \in H$. Montrer enfin que $\varphi(x) = 1$ et que $\varphi(x) = 0$, ce qui est impossible, d'où l'injectivité de θ. □

VII.2 Bases duales et antéduales

Notation 18.41 (Symbole de Kronecker)**.** *Soit* $(i,j) \in \mathbb{Z}^2$*. On note*

$$\delta_{ij} = \begin{cases} 1 & si\ i = j \\ 0 & si\ i \neq j \end{cases}.$$

Proposition 18.42. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* $(e_1,\dots,e_n)$ *une base de* E*.* $(\ell_1,\dots,\ell_n) \in (E^*)^n$ *t.q.*

$$\forall (i,j) \in [\![1,n]\!]^2,\ \ell_i(e_j) = \delta_{ij}.$$

Alors $(\ell_1,\dots,\ell_n)$ *est une base de* E^**, dite* base duale *de* $(e_1,\dots,e_n)$*, et notée* $(e_1^*,\dots,e_n^*)$*.*

Corollaire 18.43. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* $(e_1,\dots,e_n)$ *une base de* E*.*

$$\forall x \in E,\ x = \sum_{i=1}^{n} e_i^*(x) \cdot e_i. \tag{i}$$

$$\forall \varphi \in E^*,\ \varphi = \sum_{i=1}^{n} \varphi(e_i) \cdot e_i^*. \tag{ii}$$

Proposition 18.44. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* $(\ell_1,\dots,\ell_n)$ *une base de* E^**. Alors*

$$\exists!(e_1,\dots,e_n)\ \text{base de } E,\ \forall (i,j) \in [\![1,n]\!]^2,\ \ell_i(e_j) = \delta_{ij}.$$

$(e_1,\dots,e_n)$ *est dite* base antéduale *de* $(\ell_1,\dots,\ell_n)$*.*

Démonstration. Poser $\Phi : \left| \begin{array}{l} E \longrightarrow \mathbb{K}^n \\ x \longrightarrow (\ell_1(x),\dots,\ell_n(x)) \end{array} \right.$. Montrer que Φ est un isomorphisme et en déduire que les éléments de la forme $(0,\dots,0,1,0,\dots,0) \in \mathbb{K}^n$ admettent un unique antécédent par Φ, d'où le résultat. □

Proposition 18.45. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* F *un sous-espace vectoriel de* E*. On note* $n = \dim E$*,* $k = \dim F$*. Alors* F *est l'intersection de* $(\dim E - \dim F)$ *hyperplans* $(\operatorname{Ker}\varphi_1,\dots,\operatorname{Ker}\varphi_{n-k})$*, où la famille* $(\varphi_1,\dots,\varphi_{n-k})$ *est libre dans* E^**.*

Démonstration. Choisir une base $(f_1,\dots,f_k)$ de F et la compléter (à l'aide du théorème de la base incomplète) en une base $(f_1,\dots,f_n)$ de E. Montrer alors que $x = \sum_{i=1}^n \lambda_i f_i \in F \iff \forall i \in [\![k+1,n]\!],\ \lambda_i = 0 \iff x \in \bigcap_{i=k+1}^n \operatorname{Ker} f_i^*$, où $(f_1^*,\dots,f_n^*)$ est la base duale de $(f_1,\dots,f_n)$. En déduire que $F = \bigcap_{i=k+1}^n \operatorname{Ker} f_i^*$ et que $(f_{n-k+1}^*,\dots,f_n^*)$ est libre dans E^*. □

Proposition 18.46. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension* n*.* $k \in [\![0,n[\![$*. Soit* $(\varphi_1,\dots,\varphi_{n-k}) \in (E^*)^{n-k}$ *une famille libre dans* E^**. Alors* $\bigcap_{i=1}^{n-k} \operatorname{Ker}\varphi_i$ *est un sous-espace vectoriel de* E *de dimension* k*.*

Démonstration. Compléter (à l'aide du théorème de la base incomplète) $(\varphi_1,\dots,\varphi_{n-k})$ en une base $(\varphi_1,\dots,\varphi_n)$ de E^*. Soit $(e_1,\dots,e_n)$ la base antéduale de $(\varphi_1,\dots,\varphi_n)$. Montrer que $\bigcap_{i=1}^{n-k} \operatorname{Ker}\varphi_i = \operatorname{Vect}(e_{n-k+1},\dots,e_n)$ et en déduire le résultat. □

Proposition 18.47. $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel de dimension finie.* F *un sous-espace vectoriel de* E*. On note* $n = \dim E$*,* $k = \dim F$*. Soit* $(\varphi_1,\dots,\varphi_{n-k}) \in (E^*)^{n-k}$ *libre t.q.* $F = \bigcap_{i=1}^{n-k} \operatorname{Ker}\varphi_i$*. Soit* $\psi \in E^* \backslash \{0\}$*. Alors*

$$F \subset \operatorname{Ker}\psi \iff \psi \in \operatorname{Vect}(\varphi_1,\dots,\varphi_{n-k}).$$

Démonstration. ($\Rightarrow$) Compléter $(\varphi_1,\dots,\varphi_{n-k})$ en une base $(\varphi_1,\dots,\varphi_n)$ de E^*, puis écrire ψ dans la base $(\varphi_1,\dots,\varphi_n)$. □

Chapitre 19

Matrices

I Généralités

Définition 19.1 (Matrice)**.** $(n,p) \in (\mathbb{N}^*)^2$*. On appelle* matrice $n \times p$ *toute application*

$$A : \left| \begin{array}{c} [\![1,n]\!] \times [\![1,p]\!] \longrightarrow \mathbb{K} \\ (i,j) \longmapsto a_{ij} \end{array} \right. .$$

On note

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{ip} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{np} \end{pmatrix}.$$

Notation 19.2. *L'ensemble des matrices $n \times p$ est noté $\mathbb{M}_{n,p}(\mathbb{K})$. On note de plus $\mathbb{M}_n(\mathbb{K}) = \mathbb{M}_{n,n}(\mathbb{K})$.*

Vocabulaire 19.3 (Matrices lignes et colonnes)**.** *Si $A \in \mathbb{M}_{1,n}(\mathbb{K})$, alors A est dite* matrice ligne*. Si $A \in \mathbb{M}_{n,1}(\mathbb{K})$, alors A est dite* matrice colonne*.*

Notation 19.4. *Pour $(i_0, j_0) \in [\![1,n]\!] \times [\![1,p]\!]$, on note*

$$E_{i_0 j_0} = (\delta_{i,i_0}\delta_{j,j_0})_{\substack{i \in [\![1,n]\!] \\ j \in [\![1,p]\!]}} \in \mathbb{M}_{n,p}(\mathbb{K}).$$

Définition 19.5 (Addition et multiplication par un scalaire)**.** *On définit les lois $+$ et $\cdot$ par :*

$$+ : \left| \begin{array}{c} \mathbb{M}_{n,p}(\mathbb{K})^2 \longrightarrow \mathbb{M}_{n,p}(\mathbb{K}) \\ (a_{ij}), (b_{ij}) \longmapsto (a_{ij} + b_{ij}) \end{array} \right. \quad et \quad \cdot : \left| \begin{array}{c} \mathbb{K} \times \mathbb{M}_{n,p}(\mathbb{K}) \longrightarrow \mathbb{M}_{n,p}(\mathbb{K}) \\ \lambda, (a_{ij}) \longmapsto (\lambda a_{ij}) \end{array} \right. .$$

Proposition 19.6. $(\mathbb{M}_{n,p}(\mathbb{K}), +, \cdot)$ *est un $\mathbb{K}$-espace vectoriel de dimension np.*

Démonstration. Montrer que $(E_{i_0 j_0})_{\substack{i_0 \in [\![1,n]\!] \\ j_0 \in [\![1,p]\!]}}$ est une base de $\mathbb{M}_{n,p}(\mathbb{K})$. □

Définition 19.7 (Sous-matrice)**.** *$A \in \mathbb{M}_{n,p}(\mathbb{K})$. Une sous-matrice de A est une restriction de A à $I \times J$, où $I \subset [\![1,n]\!]$ et $J \subset [\![1,p]\!]$.*

Définition 19.8 (Transposée)**.** *$A = (a_{ij}) \in \mathbb{M}_{n,p}(\mathbb{K})$. On appelle* transposée *de A, notée ${}^tA$, la matrice $(a_{ji}) \in \mathbb{M}_{p,n}(\mathbb{K})$.*

Proposition 19.9. (i) *L'application* $\left|\begin{array}{c}\mathbb{M}_{n,p}(\mathbb{K}) \longrightarrow \mathbb{M}_{p,n}(\mathbb{K}) \\ A \longmapsto {}^tA\end{array}\right.$ *est linéaire.*

(ii) $\forall A \in \mathbb{M}_{n,p}(\mathbb{K}),\ {}^t({}^tA) = A$.

(iii) *Soit* $T : \left|\begin{array}{c}\mathbb{M}_n(\mathbb{K}) \longrightarrow \mathbb{M}_n(\mathbb{K}) \\ A \longmapsto {}^tA\end{array}\right.$. *Alors*

$$\mathbb{M}_n(\mathbb{K}) = \underbrace{\operatorname{Ker}\left(T - id_{\mathbb{M}_n(\mathbb{K})}\right)}_{\mathscr{S}_n(\mathbb{K})} \oplus \underbrace{\operatorname{Ker}\left(T + id_{\mathbb{M}_n(\mathbb{K})}\right)}_{\mathscr{A}_n(\mathbb{K})}.$$

Vocabulaire 19.10 (Matrices symétriques et antisymétriques)**.** *$\mathscr{S}_n(\mathbb{K})$ est dit espace vectoriel des* matrices symétriques *et $\mathscr{A}_n(\mathbb{K})$ est dit espace vectoriel des* matrices antisymétriques*.*

II Matrice d'une application linéaire

Définition 19.11 (Matrice d'un vecteur ou d'un système de vecteurs)**.** *E un $\mathbb{K}$-espace vectoriel de dimension p, $e = (e_1, \dots, e_p)$ une base de E.*

(i) *Pour $a = \sum_{i=1}^{p} x_i e_i \in E$, on note* $\operatorname{Mat}_e(a) = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{M}_{p,1}(\mathbb{K})$.

(ii) *Pour $(a_1, \dots, a_n) \in E^n$, on note* $\operatorname{Mat}_e(a_1, \dots, a_n)$ *la matrice de $\mathbb{M}_{p,n}(\mathbb{K})$ dont la j-ième colonne est* $\operatorname{Mat}_e(a_j)$ *pour tout $j \in [\![1, n]\!]$.*

Définition 19.12 (Matrice d'une application linéaire)**.** *E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. $e = (e_1, \dots, e_p)$ une base de E, $f = (f_1, \dots, f_n)$ une base de F. $u \in \mathcal{L}(E, F)$. Pour $j \in [\![1, p]\!]$, soit $(\lambda_{1j}, \dots, \lambda_{nj})$ les composantes de $u(e_j)$ dans la base f. On définit alors*

$$\operatorname{Mat}_{e,f}(u) = \begin{pmatrix} \lambda_{11} & \cdots & \lambda_{1j} & \cdots & \lambda_{1p} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \lambda_{i1} & \cdots & \lambda_{ij} & \cdots & \lambda_{ip} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \lambda_{n1} & \cdots & \lambda_{nj} & \cdots & \lambda_{np} \end{pmatrix} \in \mathbb{M}_{n,p}(\mathbb{K}).$$

Autrement dit, $\operatorname{Mat}_{e,f}(u) = \operatorname{Mat}_f(u(e_1), \dots, u(e_p))$.

Notation 19.13. *E un $\mathbb{K}$-espace vectoriel de dimension p, $e = (e_1, \dots, e_p)$ une base de E. $u \in \mathcal{L}(E)$. On notera* $\operatorname{Mat}_e(u) = \operatorname{Mat}_{e,e}(u)$.

Notation 19.14. *E un $\mathbb{K}$-espace vectoriel de dimension p. e une base de E. On note :*

(i) $I_p = \operatorname{Mat}_e(id_E) \in \mathbb{M}_p(\mathbb{K})$,

(ii) $0 = \operatorname{Mat}_e(0) \in \mathbb{M}_p(\mathbb{K})$.

Théorème 19.15. *E et F deux $\mathbb{K}$-espaces vectoriels de dimensions respectives p et n. e une base de E, f une base de F. $u \in \mathcal{L}(E,F)$. Alors u est entièrement déterminée par $\mathrm{Mat}_{e,f}(u)$. De plus, l'application*

$$\left|\begin{array}{l}\mathcal{L}(E,F) \longrightarrow \mathbb{M}_{n,p}(\mathbb{K}) \\ \qquad u \longmapsto \mathrm{Mat}_{e,f}(u)\end{array}\right.$$

est un isomorphisme d'espaces vectoriels.

Vocabulaire 19.16 (Application linéaire canoniquement associée à une matrice)**.** *e la base canonique de $\mathbb{K}^p$, f la base canonique de $\mathbb{K}^n$. $M \in \mathbb{M}_{n,p}(\mathbb{K})$. L'application linéaire $u \in \mathcal{L}(\mathbb{K}^p, \mathbb{K}^n)$ t.q. $M = \mathrm{Mat}_{e,f}(u)$ est dite* application linéaire canoniquement associée à *M.*

III Produit matriciel

Définition 19.17 (Produit matriciel)**.** *$A = (a_{ij}) \in \mathbb{M}_{n,p}(\mathbb{K})$, $B = (b_{ij}) \in \mathbb{M}_{p,q}(\mathbb{K})$. On définit*

$$AB = \left(\sum_{k=1}^{p} a_{ik}b_{kj}\right)_{\substack{i\in[\![1,n]\!] \\ j\in[\![1,q]\!]}} \in \mathbb{M}_{n,q}(\mathbb{K}).$$

Proposition 19.18. *$A \in \mathbb{M}_{n,p}(\mathbb{K}), B \in \mathbb{M}_{p,q}(\mathbb{K})$. On note $\mathfrak{L}_1, \ldots, \mathfrak{L}_n$ les n vecteurs lignes de A, $\mathfrak{C}_1, \ldots, \mathfrak{C}_q$ les q vecteurs colonnes de B. En notant $AB = (m_{ij})$, on a*

$$\forall (i,j) \in [\![1,n]\!] \times [\![1,q]\!],\ m_{ij} = \mathfrak{L}_i\mathfrak{C}_j,$$

en identifiant $\mathbb{K}$ à $\mathbb{M}_1(\mathbb{K})$.

Proposition 19.19. *E, F et G trois $\mathbb{K}$-espaces vectoriels de dimension finie. e, f et g des bases respectives de E, F et G. $u \in \mathcal{L}(E,F)$, $v \in \mathcal{L}(F,G)$.*

$$\mathrm{Mat}_{e,g}(v \circ u) = \mathrm{Mat}_{f,g}(v) \times \mathrm{Mat}_{e,f}(u).$$

Proposition 19.20. *$(A, A') \in \mathbb{M}_{n,p}(\mathbb{K})^2$, $(B, B') \in \mathbb{M}_{p,q}(\mathbb{K})^2$, $C \in \mathbb{M}_{q,r}(\mathbb{K})$, $\lambda \in \mathbb{K}$.*

(i) $A(BC) = (AB)C$,

(ii) $(A + A')B = AB + A'B$,

(iii) $A(B + B') = AB + AB'$,

(iv) $\lambda(AB) = (\lambda A)B = A(\lambda B)$.

Démonstration. Utiliser les applications linéaires canoniquement associées aux matrices, puis appliquer les propriétés des applications linéaires. □

IV Algèbre des matrices carrées

IV.1 Généralités

Proposition 19.21. *$(\mathbb{M}_n(\mathbb{K}), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel et $(\mathbb{M}_n(\mathbb{K}), +, \times)$ est un anneau. On dit que $\mathbb{M}_n(\mathbb{K})$ est une* algèbre*.*

Proposition 19.22. *$(i,j,k,\ell) \in [\![1,n]\!]^4$.*

$$E_{ij}E_{k\ell} = \delta_{jk}E_{i\ell}.$$

IV.2 Matrices particulières

Vocabulaire 19.23 (Matrices diagonales et triangulaires)**.** $A = (a_{ij}) \in \mathbb{M}_n(\mathbb{K})$.

(i) *A est dite* diagonale *lorsque* $\forall (i,j) \in [\![1,n]\!]^2,\ i \neq j \implies a_{ij} = 0$. *On note* $\mathfrak{D}_n(\mathbb{K})$ *l'ensemble des matrices diagonales.*

(ii) *A est dite* triangulaire supérieure *(resp. inférieure) lorsque* $\forall (i,j) \in [\![1,n]\!]^2,\ i > j \implies a_{ij} = 0$ *(resp.* $\forall (i,j) \in [\![1,n]\!]^2,\ i < j \implies a_{ij} = 0$*). On note* $\mathfrak{T}_n^+(\mathbb{K})$ *(resp.* $\mathfrak{T}_n^-(\mathbb{K})$*) l'ensemble des matrices triangulaires supérieures (resp. inférieures).*

(iii) *A est dite* triangulaire supérieure stricte *(resp. inférieure stricte) lorsque* $\forall (i,j) \in [\![1,n]\!]^2,\ i \geqslant j \implies a_{ij} = 0$ *(resp.* $\forall (i,j) \in [\![1,n]\!]^2,\ i \leqslant j \implies a_{ij} = 0$*). On note* $\mathfrak{T}_n^{++}(\mathbb{K})$ *(resp.* $\mathfrak{T}_n^{--}(\mathbb{K})$*) l'ensemble des matrices triangulaires supérieures strictes (resp. inférieures strictes).*

Définition 19.24 (Diagonalisabilité)**.** *E un $\mathbb{K}$-espace vectoriel de dimension finie. $u \in \mathcal{L}(E)$ est dit* diagonalisable *s'il existe e base de E t.q* $\mathrm{Mat}_e(u) \in \mathfrak{D}_n(\mathbb{K})$.

Notation 19.25. $(\gamma_1, \ldots, \gamma_n) \in \mathbb{K}^n$. *On note*

$$\mathrm{diag}(\gamma_1, \ldots, \gamma_n) = \begin{pmatrix} \gamma_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \gamma_n \end{pmatrix} \in \mathfrak{D}_n(\mathbb{K}).$$

Proposition 19.26.

(i) *$\mathfrak{D}_n(\mathbb{K})$ est un sous-espace vectoriel de $\mathbb{M}_n(\mathbb{K})$ de dimension n, et est stable par $\times$. Et de plus :*

$$\mathrm{diag}(\alpha_1, \ldots, \alpha_n) \times \mathrm{diag}(\beta_1, \ldots, \beta_n) = \mathrm{diag}(\alpha_1\beta_1, \ldots, \alpha_n\beta_n).$$

(ii) *$\mathfrak{T}_n^+(\mathbb{K})$ est un sous-espace vectoriel de $\mathbb{M}_n(\mathbb{K})$ de dimension $\frac{n(n+1)}{2}$, et est stable par $\times$.*

(iii) *$\mathscr{S}_n(\mathbb{K})$ et $\mathscr{A}_n(\mathbb{K})$ sont des sous-espaces vectoriels de $\mathbb{M}_n(\mathbb{K})$ de dimensions respectives $\frac{n(n+1)}{2}$ et $\frac{n(n-1)}{2}$.*

IV.3 Trace

Définition 19.27 (Trace)**.** *$M = (m_{ij}) \in \mathbb{M}_n(\mathbb{K})$. On définit*

$$\mathrm{tr}\, M = \sum_{i=1}^{n} m_{ii}.$$

Proposition 19.28.

(i) $\mathrm{tr} \in \mathcal{L}(\mathbb{M}_n(\mathbb{K}), \mathbb{K})$.

(ii) $\forall (A,B) \in \mathbb{M}_n(\mathbb{K})^2,\ \mathrm{tr}(AB) = \mathrm{tr}(BA)$.

(iii) $\forall A \in \mathbb{M}_n(\mathbb{K}),\ \mathrm{tr}\left({}^tA\right) = \mathrm{tr}\, A$.

IV.4 Transposition et produit

Proposition 19.29. $\forall (A,B) \in \mathbb{M}_n(\mathbb{K})^2,\ {}^t(AB) = {}^tB\,{}^tA$.

V Applications linéaires et matrices

Proposition 19.30. *E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. e une base de E, f une base de F. $u \in \mathcal{L}(E,F)$.*

$$\forall x \in E,\ \mathrm{Mat}_f\left(u(x)\right) = \mathrm{Mat}_{e,f}(u) \times \mathrm{Mat}_e(x).$$

Proposition 19.31. *$A \in \mathbb{M}_{n,p}(\mathbb{K})$. Alors l'application linéaire canoniquement associée à A est*

$$u : \left| \begin{array}{l} \mathbb{K}^p \longrightarrow \mathbb{K}^n \\ X \longmapsto AX \end{array} \right. ,$$

en identifiant $\mathbb{K}^p$ à $\mathbb{M}_{p,1}(\mathbb{K})$ et $\mathbb{K}^n$ à $\mathbb{M}_{n,1}(\mathbb{K})$.

Corollaire 19.32. *E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. e une base de E, f une base de F. $u \in \mathcal{L}(E,F)$. $(x,y) \in E \times F$. $A = \mathrm{Mat}_{e,f}(u)$, $X = \mathrm{Mat}_e(x)$ et $Y = \mathrm{Mat}_f(y)$.*

(i) $x \in \operatorname{Ker} u \iff AX = 0$.

(ii) $y \in \operatorname{Im} u \iff \exists U \in \mathrm{Mat}_{p,1}(\mathbb{K}),\ Y = AU$.

VI Matrices carrées inversibles

VI.1 Généralités

Définition 19.33 (Matrices inversibles)**.** *$A \in \mathbb{M}_n(\mathbb{K})$ est dite* inversible *lorsqu'il existe $B \in \mathbb{M}_n(\mathbb{K})$ t.q. $AB = BA = I_n$. On note alors $A^{-1} = B$.*

Notation 19.34. *L'ensemble des matrices inversibles est noté $GL_n(\mathbb{K})$.*

Proposition 19.35.

(i) *Pour $A \in \mathbb{M}_n(\mathbb{K})$, A^{-1} est déterminée de manière unique si elle existe.*

(ii) *$(GL_n(\mathbb{K}), \times)$ est un groupe isomorphe à $(GL(\mathbb{K}^n), \circ)$.*

Proposition 19.36. *$A \in \mathbb{M}_n(\mathbb{K})$. A est inversible* ssi *${}^tA$ est inversible. Et dans ce cas, $\left({}^tA\right)^{-1} = {}^t\left(A^{-1}\right)$.*

Proposition 19.37. *$A \in \mathbb{M}_n(\mathbb{K})$. E un $\mathbb{K}$-espace vectoriel de dimension n. e une base de E. $u \in \mathcal{L}(E)$ t.q. $\mathrm{Mat}_e(u) = A$. On note $\mathfrak{L}_1, \ldots, \mathfrak{L}_n$ les n vecteurs lignes de A, $\mathfrak{C}_1, \ldots, \mathfrak{C}_n$ les n vecteurs colonnes de A.*

$$\begin{aligned}
A \text{ inversible} &\iff u \text{ isomorphisme} && \text{(i)}\\
&\iff A \text{ inversible à gauche} && \text{(ii)}\\
&\iff A \text{ inversible à droite} && \text{(iii)}\\
&\iff \left(\forall X \in \mathbb{M}_n(\mathbb{K}),\ AX = 0 \Rightarrow X = 0\right) && \text{(iv)}\\
&\iff \left(\forall Y \in \mathbb{M}_n(\mathbb{K}),\ \exists! X \in \mathbb{M}_n(\mathbb{K}),\ Y = AX\right) && \text{(v)}\\
&\iff \left(\mathfrak{C}_1, \ldots, \mathfrak{C}_n\right) \text{ est libre dans } \mathbb{K}^n && \text{(vi)}\\
&\iff \left(\mathfrak{L}_1, \ldots, \mathfrak{L}_n\right) \text{ est libre dans } \mathbb{K}^n && \text{(vii)}\\
&\iff \operatorname{rg} u = n. && \text{(viii)}
\end{aligned}$$

Proposition 19.38. *$A \in \mathbb{M}_n(\mathbb{K})$. E et F deux $\mathbb{K}$-espaces vectoriels de dimension n. e une base de E, f une base de F. $v \in \mathcal{L}(E,F)$ t.q. $\mathrm{Mat}_{e,f}(v) = A$. Alors A est inversible* ssi *v est un isomorphisme. Et dans ce cas, $A^{-1} = \mathrm{Mat}_{f,e}\left(v^{-1}\right)$.*

Proposition 19.39. $(a,b,c,d) \in \mathbb{K}^4$. *Si* $ad \neq bc$, *alors*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

VI.2 Opérations élémentaires sur les lignes et les colonnes

Proposition 19.40. $A \in \mathbb{M}_n(\mathbb{K})$.

(i) $E_{ij}A$ *est la matrice dont la* i*-ième ligne est la* j*-ième ligne de* A, *les autres étant nulles.*

(ii) AE_{ij} *est la matrice dont la* j*-ième colonne est la* i*-ième colonne de* A, *les autres étant nulles.*

Démonstration. Écrire A dans la base $(E_{k\ell})_{\substack{k\in[\![1,n]\!] \\ \ell\in[\![1,n]\!]}}$ et utiliser la proposition 19.22. □

Définition 19.41 (Matrices élémentaires)**.** $\lambda \in \mathbb{K}^*$. $(i,j) \in [\![1,n]\!]^2$.

(i) *Pour* $i \neq j$, *la* matrice de transvection $T_{ij}(\lambda) \in \mathbb{M}_n(\mathbb{K})$ *est définie par*

$$T_{ij}(\lambda) = I_n + \lambda E_{ij}.$$

(ii) *La* matrice de dilatation $D_i(\lambda) \in \mathbb{M}_n(\mathbb{K})$ *est définie par*

$$D_i(\lambda) = I_n + (\lambda - 1)E_{ii}.$$

(iii) *Pour* $i \neq j$, *la* matrice de transposition $P_{ij} \in \mathbb{M}_n(\mathbb{K})$ *est définie par*

$$P_{ij} = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}.$$

Proposition 19.42. *Les matrices de transvection, de dilatation et de transposition sont inversibles et :*

$$(T_{ij}(\lambda))^{-1} = T_{ij}(-\lambda) \quad et \quad (D_i(\lambda))^{-1} = D_i\left(\frac{1}{\lambda}\right) \quad et \quad (P_{ij})^{-1} = P_{ij}.$$

Proposition 19.43. $A \in \mathbb{M}_{n,p}(\mathbb{K})$. $\lambda \in \mathbb{K}^*$, $(i,j) \in [\![1,n]\!]^2$. *On note* $\mathfrak{L}_1, \ldots, \mathfrak{L}_n$ *les* n *vecteurs lignes de* A, $\mathfrak{C}_1, \ldots, \mathfrak{C}_n$ *les* n *vecteurs colonnes de* A. *On a alors une correspondance entre les matrices élémentaires et les opérations élémentaires sur les lignes et les colonnes de* A *(c.f. définition 4.6) :*

Lignes	Transvection	$\mathfrak{L}_i \longleftarrow \mathfrak{L}_i + \lambda\mathfrak{L}_j$	$A \longmapsto T_{ij}(\lambda)A$
	Dilatation	$\mathfrak{L}_i \longleftarrow \lambda\mathfrak{L}_i$	$A \longmapsto D_i(\lambda)A$
	Transposition	$\mathfrak{L}_i \longleftrightarrow \mathfrak{L}_j$	$A \longmapsto P_{ij}A$
Colonnes	Transvection	$\mathfrak{C}_i \longleftarrow \mathfrak{C}_i + \lambda\mathfrak{C}_j$	$A \longmapsto AT_{ji}(\lambda)$
	Dilatation	$\mathfrak{C}_i \longleftarrow \lambda\mathfrak{C}_i$	$A \longmapsto AD_i(\lambda)$
	Transposition	$\mathfrak{C}_i \longleftrightarrow \mathfrak{C}_j$	$A \longmapsto AP_{ij}$

VI.3 Cas des matrices triangulaires

Proposition 19.44. $A = (a_{ij}) \in \mathfrak{T}_n^+(\mathbb{K})$ *(ou* $\mathfrak{T}_n^-(\mathbb{K})$*). Alors* A *est inversible* ssi $\forall i \in [\![1,n]\!]$, $a_{ii} \neq 0$.

VII Rang d'une matrice

VII.1 Définition

Définition 19.45 (Rang)**.** $A = \begin{bmatrix} \mathfrak{C}_1 & \cdots & \mathfrak{C}_p \end{bmatrix} \in \mathbb{M}_{n,p}(\mathbb{K})$. *On définit*

$$\operatorname{rg} A = \dim \operatorname{Vect}(\mathfrak{C}_1, \ldots, \mathfrak{C}_p).$$

Proposition 19.46. *E un $\mathbb{K}$-espace vectoriel de dimension n, e une base de E. $(x_1, \ldots, x_p) \in E^p$.*

$$\operatorname{rg}(x_1, \ldots, x_p) = \operatorname{rg} \operatorname{Mat}_e(x_1, \ldots, x_p).$$

Proposition 19.47. *E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. e une base de E, f une base de F. $u \in \mathcal{L}(E, F)$.*

$$\operatorname{rg} u = \operatorname{rg} \operatorname{Mat}_{e,f}(u).$$

Corollaire 19.48. *$A \in \mathbb{M}_{n,p}(\mathbb{K})$, $B \in \mathbb{M}_{p,q}(\mathbb{K})$.*

(i) $\operatorname{rg} A \leqslant \min(n, p)$.

(ii) $\operatorname{rg}(AB) \leqslant \min(\operatorname{rg} A, \operatorname{rg} B)$.

(iii) *Si $n = p$, alors $A \in GL_n(\mathbb{K}) \iff \operatorname{rg} A = n$.*

(iv) *La multiplication à droite ou à gauche par une matrice inversible ne modifie pas le rang.*

VII.2 Calcul du rang

Proposition 19.49. *$\alpha \in \mathbb{K}^*$.*

$$\operatorname{rg} \begin{pmatrix} \alpha & 0 & \cdots & 0 \\ \vdots & & A' & \\ \vdots & & & \end{pmatrix} = 1 + \operatorname{rg} A'.$$

Démonstration. En notant $\mathfrak{C}_1, \ldots, \mathfrak{C}_p$ les vecteurs colonnes de A, utiliser le fait que $\operatorname{Vect}(\mathfrak{C}_1, \ldots, \mathfrak{C}_p) = \operatorname{Vect}(\mathfrak{C}_1) \oplus \operatorname{Vect}(\mathfrak{C}_2, \ldots, \mathfrak{C}_p)$. □

VIII Changement de base

VIII.1 Matrice de passage

Définition 19.50 (Matrice de passage)**.** *E un $\mathbb{K}$-espace vectoriel de dimension finie. $e = (e_1, \ldots, e_n)$ et $f = (f_1, \ldots, f_n)$ deux bases de E. On note*

$$P_e^f = \operatorname{Mat}_e(f_1, \ldots, f_n).$$

Proposition 19.51. *E un $\mathbb{K}$-espace vectoriel de dimension n. e, f, g trois bases de E.*

(i) $P_e^f = \operatorname{Mat}_{f,e}(id_E)$.

(ii) $P_e^f \in GL_n(\mathbb{K})$ *et* $\left(P_e^f\right)^{-1} = P_f^e$.

(iii) $P_e^g = P_e^f P_f^g$.

Proposition 19.52. *E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. e une base de E, f une base de F. $u \in \mathcal{L}(E, F)$ un isomorphisme. Alors* $\operatorname{Mat}_{e,f}(u) = P_f^{u(e)}$.

VIII.2 Formules de changement de base

Proposition 19.53. *E un $\mathbb{K}$-espace vectoriel de dimension finie, e et e' deux bases de E. $x \in E$. Alors*

$$\mathrm{Mat}_e(x) = P_e^{e'} \times \mathrm{Mat}_{e'}(x).$$

Proposition 19.54. *E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. e, e' bases de E, f, f' bases de F. $u \in \mathcal{L}(E,F)$.*

$$\mathrm{Mat}_{e,f}(u) = P_f^{f'} \times \mathrm{Mat}_{e',f'}(u) \times \left(P_e^{e'}\right)^{-1}.$$

Corollaire 19.55. *E un $\mathbb{K}$-espace vectoriel de dimension finie, e et e' deux bases de E. $\psi \in \mathcal{L}(E,\mathbb{K})$, $u \in \mathcal{L}(E)$.*

(i) $\mathrm{Mat}_{e,1}(\psi) = \mathrm{Mat}_{e',1}(\psi) \times \left(P_e^{e'}\right)^{-1}$.

(ii) $\mathrm{Mat}_e(u) = P_e^{e'} \times \mathrm{Mat}_{e'}(u) \times \left(P_e^{e'}\right)^{-1}$.

VIII.3 Matrices semblables

Définition 19.56 (Matrices semblables)**.** *$(A,B) \in \mathbb{M}_n(\mathbb{K})^2$. On dit que A et B sont* semblables *lorsque $\exists P \in GL_n(\mathbb{K})$, $A = PBP^{-1}$.*

Proposition 19.57. *$(A,B) \in \mathbb{M}_n(\mathbb{K})^2$. A et B sont semblables* ssi *A et B sont les matrices d'un même endomorphisme dans deux bases éventuellement différentes.*

Proposition 19.58. *"Être semblable à" est une relation d'équivalence.*

Proposition 19.59. *A et B deux matrices semblables.*

(i) $\mathrm{tr}\, A = \mathrm{tr}\, B$,

(ii) $\mathrm{rg}\, A = \mathrm{rg}\, B$.

Proposition 19.60. *A et B deux matrices semblables t.q. $A = PBP^{-1}$, avec $P \in GL_n(\mathbb{K})$.*

(i) $\forall k \in \mathbb{N}$, $A^k = PB^kP^{-1}$.

(ii) ${}^tA$ *et* ${}^tB$ *sont semblables.*

(iii) *Si A et B sont inversibles alors A^{-1} et B^{-1} sont semblables.*

VIII.4 Trace d'un endomorphisme

Définition 19.61 (Trace d'un endomorphisme)**.** *E un $\mathbb{K}$-espace vectoriel de dimension finie, e une base de E. $u \in \mathcal{L}(E)$. On définit*

$$\mathrm{tr}\, u = \mathrm{tr}\, \mathrm{Mat}_e(u).$$

Proposition 19.62. *L'application* $\left|\begin{array}{ccc} \mathcal{L}(E) & \longrightarrow & \mathbb{K} \\ u & \longmapsto & \mathrm{tr}\, u \end{array}\right.$ *est une forme linéaire.*

IX Polynômes de matrices et d'endomorphismes

IX.1 Généralités

Définition 19.63 (Polynômes de matrices et d'endomorphismes)**.** *Soit* $P = \sum_{k\in\mathbb{N}} \lambda_k X^k \in \mathbb{K}[X]$, $u \in \mathcal{L}(E)$, $A \in \mathbb{M}_n(\mathbb{K})$. *On définit :*

(i) $P(u) = \sum_{k\in\mathbb{N}} \lambda_k u^k \in \mathcal{L}(E)$.

(ii) $P(A) = \sum_{k\in\mathbb{N}} \lambda_k A^k \in \mathbb{M}_n(\mathbb{K})$.

Proposition 19.64. $u \in \mathcal{L}(E)$. *L'application* $\left|\begin{array}{c}\mathbb{K}[X] \longrightarrow \mathcal{L}(E) \\ P \longmapsto P(u)\end{array}\right.$ *est linéaire, et de plus :*

$$\forall (P,Q) \in \mathbb{K}[X]^2,\ P(u)\circ Q(u) = (PQ)(u) = (QP)(u) = Q(u)\circ P(u).$$

IX.2 Stabilité et polynômes

Proposition 19.65. $(u,v) \in \mathcal{L}(E)^2$ *t.q.* $u\circ v = v\circ u$. *Alors* $\operatorname{Im} v$ *et* $\operatorname{Ker} v$ *sont stables par* u.

Corollaire 19.66. $u \in \mathcal{L}(E)$, $P \in \mathbb{K}[X]$. *Alors* $\operatorname{Im} P(u)$ *et* $\operatorname{Ker} P(u)$ *sont stables par* u.

Notation 19.67. *Pour* $u \in \mathcal{L}(E)$, *on notera* $\mathfrak{J}_u = \{P \in \mathbb{K}[X],\ P(u) = 0\}$.

Proposition 19.68. $u \in \mathcal{L}(E)$. *Alors* $\mathfrak{J}_u$ *est un idéal de* $\mathbb{K}[X]$.

Définition 19.69 (Polynôme minimal annulateur)**.** $u \in \mathcal{L}(E)$. *Alors* $\exists \mu_u \in \mathbb{K}[X]$, $\mathfrak{J}_u = \mu_u \mathbb{K}[X]$. *Si* $\mathfrak{J}_u \neq \{0\}$, *alors* μ_u^* *est dit* le polynôme minimal annulateur *de* u.

Proposition 19.70. E *un* $\mathbb{K}$*-espace vectoriel de dimension finie,* $u \in \mathcal{L}(E)$. *Alors* $\mathfrak{J}_u \neq \{0\}$.

Démonstration. Voir proposition 20.16. □

IX.3 Lemme des noyaux

Lemme 19.71 (Lemme des noyaux)**.** $u \in \mathcal{L}(E)$.

$$\forall (P_1,P_2) \in \mathbb{K}[X]^2,\ P_1 \wedge P_2 = 1 \Longrightarrow \operatorname{Ker}(P_1P_2)(u) = \operatorname{Ker} P_1(u) \oplus \operatorname{Ker} P_2(u). \quad \text{(i)}$$

$$\forall (P_1,\dots,P_n) \in \mathbb{K}[X]^n,\ \Big[\forall (i,j) \in [\![1,n]\!]^2,\ i \neq j \Rightarrow P_i \wedge P_j = 1\Big] \Longrightarrow \operatorname{Ker}\left[\left(\prod_{i=1}^n P_i\right)(u)\right] = \bigoplus_{i=1}^n \operatorname{Ker} P_i(u). \quad \text{(ii)}$$

Démonstration. (i) Soit $(P_1,P_2) \in \mathbb{K}[X]^2$ t.q. $P_1 \wedge P_2 = 1$. En appliquant l'égalité de Bézout, obtenir l'existence de $(U,V) \in \mathbb{K}[X]^2$ t.q. $UP_1 + VP_2 = 1$. En déduire $\forall x \in \operatorname{Ker}(P_1P_2)(u)$, $\underbrace{[U(u)\circ P_1(u)](x)}_{x_1} + \underbrace{[V(u)\circ P_2(u)](x)}_{x_2} = x$. Montrer que $x_1 \in \operatorname{Ker} P_2(u)$, $x_2 \in \operatorname{Ker} P_1(u)$ et en déduire que $\operatorname{Ker}(P_1P_2)(u) = \operatorname{Ker} P_1(u) + \operatorname{Ker} P_2(u)$. Montrer alors que $\operatorname{Ker} P_1(u) \cap \operatorname{Ker} P_2(u) = \{0\}$ et en déduire que la somme est directe. (ii) Par récurrence. □

X Matrices blocs

X.1 Généralités

Notation 19.72 (Matrices blocs)**.** *Pour $(i,j) \in [\![1,a]\!] \times [\![1,b]\!]$, soit $A_{ij} \in \mathbb{M}_{n_i p_j}(\mathbb{K})$. On note alors*

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1b} \\ \vdots & \ddots & \vdots \\ A_{a1} & \cdots & A_{ab} \end{pmatrix} \in \mathbb{M}_{np}(\mathbb{K}),$$

où $n = \sum_{i=1}^{a} n_i$, $p = \sum_{j=1}^{b} p_j$.

Proposition 19.73. *Soit $A = (A_{ij}) \in \mathbb{M}_{n,p}(\mathbb{K})$ et $B = (B_{ij}) \in \mathbb{M}_{n,p}(\mathbb{K})$ deux matrices écrites sous forme de blocs, $(\lambda,\mu) \in \mathbb{K}^2$.*

$$\lambda \begin{pmatrix} A_{11} & \cdots & A_{1b} \\ \vdots & \ddots & \vdots \\ A_{a1} & \cdots & A_{ab} \end{pmatrix} + \mu \begin{pmatrix} B_{11} & \cdots & B_{1b} \\ \vdots & \ddots & \vdots \\ B_{a1} & \cdots & B_{ab} \end{pmatrix}$$
$$= \begin{pmatrix} \lambda A_{11} + \mu B_{11} & \cdots & \lambda A_{1b} + \mu B_{1b} \\ \vdots & \ddots & \vdots \\ \lambda A_{a1} + \mu B_{a1} & \cdots & \lambda A_{ab} + \mu B_{ab} \end{pmatrix}.$$

Proposition 19.74. *E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie, avec $E = \bigoplus_{i=1}^{b} E_i$, $F = \bigoplus_{j=1}^{a} F_j$. e et f bases respectives de E et F adaptées aux sommes directes $\bigoplus_{i=1}^{b} E_i$ et $\bigoplus_{j=1}^{a} F_j$. $u \in \mathcal{L}(E,F)$. $A = (A_{ij}) = \mathrm{Mat}_{e,f}(u)$ écrite sous forme de blocs. Alors*

$$A_{ij} = \mathrm{Mat}_{e_i,f_j}(p_j \circ u_{|E_i}),$$

où p_j est la projection sur F_j parallèlement à $\bigoplus_{\substack{j'=1 \\ j' \neq j}}^{a} F_{j'}$.

X.2 Produits par blocs

Proposition 19.75. *Soit $A = (A_{ij}) \in \mathbb{M}_{n,p}(\mathbb{K})$ et $B = (B_{ij}) \in \mathbb{M}_{p,q}(\mathbb{K})$ deux matrices écrites sous forme de blocs.*

$$\begin{pmatrix} A_{11} & \cdots & A_{1b} \\ \vdots & \ddots & \vdots \\ A_{a1} & \cdots & A_{ab} \end{pmatrix} \begin{pmatrix} B_{11} & \cdots & B_{1c} \\ \vdots & \ddots & \vdots \\ B_{b1} & \cdots & B_{bc} \end{pmatrix}$$
$$= \begin{pmatrix} \sum_{k=1}^{b} A_{1k}B_{k1} & \cdots & \sum_{k=1}^{b} A_{1k}B_{kc} \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^{b} A_{ak}B_{k1} & \cdots & \sum_{k=1}^{b} A_{ak}B_{kc} \end{pmatrix}.$$

XI Matrices équivalentes et conséquences

XI.1 Définition

Définition 19.76 (Matrices équivalentes)**.** $(A,B) \in \mathbb{M}_{n,p}(\mathbb{K})^2$. *On dit que A et B sont* équivalentes *lorsque $\exists (P,Q) \in GL_p(\mathbb{K}) \times GL_n(\mathbb{K})$, $A = QBP^{-1}$.*

Proposition 19.77. *E et F deux $\mathbb{K}$-espaces vectoriels de dimensions respectives p et n. e une base de E, f une base de F. $u \in \mathcal{L}(E,F)$. $M \in \mathbb{M}_{n,p}(\mathbb{K})$. Alors M est équivalente à $\mathrm{Mat}_{e,f}(u)$* ssi

$$\exists e' \text{ base de } E,\ \exists f' \text{ base de } F,\ M = \mathrm{Mat}_{e',f,'}(u).$$

XI.2 Rang et transposition

Notation 19.78. *On note* $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{M}_{n,p}(\mathbb{K})$.

Proposition 19.79. *$A \in \mathbb{M}_{n,p}(\mathbb{K})$. Alors A et $J_{\mathrm{rg}\,A}$ sont équivalentes.*

Démonstration. Soit $u \in \mathcal{L}(\mathbb{K}^p, \mathbb{K}^n)$ l'application linéaire canoniquement associée à A. En notant $r = \mathrm{rg}\,A$, choisir $(e'_{r+1}, \dots, e'_p)$ base de $\mathrm{Ker}\,u$, puis compléter cette base en $(e'_1, \dots, e'_p)$ base de $\mathbb{K}^p$. Poser alors $f'_i = u(e'_i)$ pour $i \in [\![1, r]\!]$ et compléter cette base en une base $(f'_1, \dots, f'_n)$ de $\mathbb{K}^n$. Vérifier alors que $\mathrm{Mat}_{e',f'}(u) = J_r$. □

Proposition 19.80. $\mathrm{rg}\,{}^tJ_r = \mathrm{rg}\,J_r = r$.

Corollaire 19.81. *$A \in \mathbb{M}_{n,p}(\mathbb{K})$.*

$$\mathrm{rg}\,A = \mathrm{rg}\,{}^tA.$$

Corollaire 19.82. *$A \in \mathbb{M}_{n,p}(\mathbb{K})$. $\mathfrak{L}_1, \dots, \mathfrak{L}_n$ les n vecteurs lignes de A. Alors* $\mathrm{rg}\,A = \mathrm{rg}(\mathfrak{L}_1, \dots, \mathfrak{L}_n)$.

XI.3 Rang et matrices extraites

Proposition 19.83. *$A \in \mathbb{M}_{n,p}(\mathbb{K})$. Alors* $\mathrm{rg}\,A$ *est l'ordre maximal des sous-matrices carrées inversibles de A.*

Chapitre 20

Réduction d'Endomorphismes et de Matrices

I Sous-espaces vectoriels stables

I.1 Généralités

Vocabulaire 20.1 (Sous-espace vectoriel stable)**.** *$u \in \mathcal{L}(E)$, F sous-espace vectoriel de E. F est dit* stable *par E lorsque $u(F) \subset F$.*

Proposition 20.2. *L'intersection et la somme de deux sous-espaces vectoriels stables par un endomorphisme sont stables par cet endomorphisme.*

Définition 20.3 (Éléments propres d'un endomorphisme)**.** *$u \in \mathcal{L}(E)$.*

(i) *On dit que $x \in E$ est un* vecteur propre *de u lorsque $x \neq 0$ et $\mathrm{Vect}(x)$ est stable par u (i.e. $x \neq 0$ et $u(x)$ colinéaire à x).*

(ii) *On dit que $\lambda \in \mathbb{K}$ est une* valeur propre *de u lorsque $\exists x \in E \backslash \{0\}$, $u(x) = \lambda x$.*

(iii) *On note $\mathrm{Sp}_{\mathbb{K}}(u)$ l'ensemble des valeurs propres de u.*

(iv) *Pour $\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)$, on appelle* espace propre *associé à λ l'ensemble $E_\lambda = \mathrm{Ker}(u - \lambda id_E)$.*

Proposition 20.4. *Pour $u \in \mathcal{L}(E)$, $\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)$, E_λ est stable par u.*

I.2 Propriétés des espaces propres

Proposition 20.5. *$u \in \mathcal{L}(E)$. $(\lambda_1, \ldots, \lambda_s) \in \mathrm{Sp}_{\mathbb{K}}(u)^s$ avec $\forall (i,j) \in [\![1, s]\!]^2$, $i \neq j \implies \lambda_i \neq \lambda_j$.*

(i) *La somme $E_{\lambda_1} + E_{\lambda_2}$ est directe.*

(ii) *La somme $\sum_{i=1}^{s} E_{\lambda_i}$ est directe.*

Corollaire 20.6. *E un $\mathbb{K}$-espace vectoriel de dimension finie. Alors $u \in \mathcal{L}(E)$ admet au plus $(\dim E)$ valeurs propres.*

I.3 Version matricielle

Définition 20.7 (Éléments propres d'une matrice)**.** $A \in \mathbb{M}_n(\mathbb{K})$.

(i) *On dit que* $X \in \mathbb{M}_{n,1}(\mathbb{K})$ *est un* vecteur propre *de* A *lorsque* $X \neq 0$ *et* $\exists \lambda \in \mathbb{K}$, $AX = \lambda X$.

(ii) *On dit que* $\lambda \in \mathbb{K}$ *est une* valeur propre *de* A *si* $\exists X \in \mathbb{M}_{n,1}(\mathbb{K}) \setminus \{0\}$, $AX = \lambda X$.

(iii) *On note* $\mathrm{Sp}_{\mathbb{K}}(A)$ *l'ensemble des valeurs propres de* A.

(iv) *Pour* $\lambda \in \mathrm{Sp}_{\mathbb{K}}(A)$, *on appelle* espace propre *associé à* λ *l'ensemble* $E_\lambda = \{X \in \mathbb{M}_{n,1}(\mathbb{K}),\ AX = \lambda X\}$.

Proposition 20.8. *E un $\mathbb{K}$-espace vectoriel de dimension finie. e une base de E. $u \in \mathcal{L}(E)$. $A = \mathrm{Mat}_e(u)$. $\lambda \in \mathbb{K}$.*

(i) $\mathrm{Sp}_{\mathbb{K}}(A) = \mathrm{Sp}_{\mathbb{K}}(u)$.

(ii) $\lambda \in \mathrm{Sp}_{\mathbb{K}}(A) \iff (A - \lambda I)$ *non inversible* $\iff \mathrm{rg}(u - \lambda id_E) < n$.

II Diagonalisabilité

Définition 20.9 (Diagonalisabilité d'un endomorphisme)**.** *E un $\mathbb{K}$-espace vectoriel de dimension finie. $u \in \mathcal{L}(E)$ est dit* diagonalisable *s'il existe e base de E t.q* $\mathrm{Mat}_e(u) \in \mathfrak{D}_n(\mathbb{K})$.

Proposition 20.10. *$u \in \mathcal{L}(E)$.*

$$u \text{ diagonalisable} \iff \text{il existe une base de } E \text{ constituée de vecteurs propres de } u \tag{i}$$

$$\iff E = \bigoplus_{\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)} E_\lambda \tag{ii}$$

$$\iff \dim E = \sum_{\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)} \dim E_\lambda. \tag{iii}$$

Proposition 20.11. *E un $\mathbb{K}$-espace vectoriel de dimension finie. Si $u \in \mathcal{L}(E)$ a $(\dim E)$ valeurs propres alors u est diagonalisable et chaque espace propre de u est de dimension 1.*

Définition 20.12 (Diagonalisabilité d'une matrice)**.** $A \in \mathbb{M}_n(\mathbb{K})$ *est dite* diagonalisable *lorsque A est semblable à une matrice diagonale.*

Proposition 20.13. *E un $\mathbb{K}$-espace vectoriel de dimension finie. e une base de E. $u \in \mathcal{L}(E)$. Alors u est diagonalisable* ssi $\mathrm{Mat}_e(u)$ *est diagonalisable.*

III Diagonalisation et polynômes d'endomorphismes

Notation 20.14. *$u \in \mathcal{L}(E)$. On note* $\mathbb{K}[u] = \{Q(u),\ Q \in \mathbb{K}[X]\}$.

Proposition 20.15. *$u \in \mathcal{L}(E)$. $\mathbb{K}[u]$ est un sous-espace vectoriel de $\mathcal{L}(E)$ et un sous-anneau de $\mathcal{L}(E)$.*

Proposition 20.16. *E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$. On considère l'application*

$$\Phi_u : \left| \begin{array}{c} \mathbb{K}[X] \longrightarrow \mathbb{K}[u] \\ P \longmapsto P(u) \end{array} \right. .$$

Alors Φ_u est une application linéaire, un morphisme d'anneaux et Φ_u est non injective.

Corollaire 20.17. *E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$. Alors $\mathfrak{J}_u = \{P \in \mathbb{K}[X],\ P(u) = 0\} \neq \{0\}$.*

Proposition 20.18. *E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$. $P \in \mathfrak{J}_u \backslash \{0\}$. Alors $\mathrm{Sp}_{\mathbb{K}}(u) \subset \{\alpha \in \mathbb{K},\ P(\alpha) = 0\}$.*

Théorème 20.19. *E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$. u est diagonalisable* ssi *il existe un polynôme $P \in \mathbb{K}[X]$ scindé sur $\mathbb{K}$ et à racines simples t.q. $P(u) = 0$.*

Démonstration. ($\Rightarrow$) Vérifier que $P = \prod_{\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)} (X - \lambda)$ convient. ($\Leftarrow$) Appliquer le lemme des noyaux (lemme 19.71). □

Proposition 20.20. *E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$ diagonalisable. Pour $\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)$, on appelle p_λ la projection sur E_λ parallèlement à $\bigoplus_{\substack{\mu \in \mathrm{Sp}_{\mathbb{K}}(u) \\ \mu \neq \lambda}} E_\mu$. Alors*

$$\forall \lambda \in \mathrm{Sp}_{\mathbb{K}}(u),\ p_\lambda \in \mathbb{K}[u].$$

Démonstration. Pour $\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)$, poser

$$L_\lambda = \frac{\prod_{\substack{\mu \in \mathrm{Sp}_{\mathbb{K}}(u) \\ \mu \neq \lambda}} (X - \mu)}{\prod_{\substack{\mu \in \mathrm{Sp}_{\mathbb{K}}(u) \\ \mu \neq \lambda}} (\lambda - \mu)} \in \mathbb{K}[X]$$

(i.e. $L_\lambda(\lambda) = 1$ et $L_\lambda(\mu) = 0$ pour $\mu \neq \lambda$). Vérifier alors que $p_\lambda = L_\lambda(u)$. □

Proposition 20.21. *E un $\mathbb{K}$-espace vectoriel de dimension finie, $(u, v) \in \mathcal{L}(E)^2$.*

(i) *Soit F un sous-espace vectoriel de E stable par u. On définit $\hat{u} : \left| \begin{array}{c} F \longrightarrow F \\ x \longmapsto u(x) \end{array} \right.$. Si u est diagonalisable alors $\hat{u}$ est diagonalisable.*

(ii) *Si u et v sont diagonalisables et $u \circ v = v \circ u$, alors il existe une base de E constituée de vecteurs propres communs à u et v.*

Démonstration. (i) Appliquer le théorème 20.19. (ii) Comme u est diagonalisable, on a $E = \bigoplus_{\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)} E_\lambda(u)$ (on note ici $E_\lambda(u) = \mathrm{Ker}(u - \lambda id_E)$). Soit $\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)$. Justifier que $E_\lambda(u)$ est stable par v, puis poser $w_\lambda : \left| \begin{array}{c} E_\lambda(u) \longrightarrow E_\lambda(u) \\ x \longmapsto v(x) \end{array} \right.$. Appliquer (i) pour en déduire que w_λ est diagonalisable. Donc $E_\lambda(u) = \bigoplus_{\mu \in \mathrm{Sp}_{\mathbb{K}}(w_\lambda)} E_\mu(w_\lambda) = \bigoplus_{\mu \in \mathrm{Sp}_{\mathbb{K}}(w_\lambda)} (E_\lambda(u) \cap E_\mu(v))$. Donc

$$E = \bigoplus_{\substack{\lambda \in \mathrm{Sp}_{\mathbb{K}}(u) \\ \mu \in \mathrm{Sp}_{\mathbb{K}}(w_\lambda)}} (E_\lambda(u) \cap E_\mu(v)) \subset \sum_{\substack{\lambda \in \mathrm{Sp}_{\mathbb{K}}(u) \\ \mu \in \mathrm{Sp}_{\mathbb{K}}(v)}} (E_\lambda(u) \cap E_\mu(v)) \subset E,$$

d'où $E = \sum_{\substack{\lambda \in \mathrm{Sp}_{\mathbb{K}}(u) \\ \mu \in \mathrm{Sp}_{\mathbb{K}}(v)}} (E_\lambda(u) \cap E_\mu(v))$. Montrer alors que la somme est directe, d'où $E = \bigoplus_{\substack{\lambda \in \mathrm{Sp}_{\mathbb{K}}(u) \\ \mu \in \mathrm{Sp}_{\mathbb{K}}(v)}} (E_\lambda(u) \cap E_\mu(v))$, puis en déduire le résultat. □

Chapitre 21

Groupe Symétrique

I Généralités

Notation 21.1. *Pour $X \neq \varnothing$, on note $\mathfrak{S}_X$ l'ensemble des bijections $X \to X$ (dites aussi permutations).*

Proposition 21.2. *$(\mathfrak{S}_X, \circ)$ est un groupe en général non commutatif.*

Proposition 21.3. *Si deux ensembles X et Y sont en bijection alors $\mathfrak{S}_X$ et $\mathfrak{S}_Y$ sont isomorphes.*

Notation 21.4. *Pour $n \in \mathbb{N}^*$, on note $\mathfrak{S}_n = \mathfrak{S}_{[\![1,n]\!]}$.*

Proposition 21.5.

(i) $\operatorname{card} \mathfrak{S}_n = n!$.

(ii) $\mathfrak{S}_n$ *est commutatif* ssi $n \leqslant 2$.

Notation 21.6. *$s \in \mathfrak{S}_n$. On notera $s = \begin{pmatrix} 1 & 2 & \cdots & n \\ s(1) & s(2) & \cdots & s(n) \end{pmatrix}$, en omettant éventuellement les points fixes de s.*

Notation 21.7. *Pour $n \geqslant 3$, on notera $(i\,j) = \begin{pmatrix} i & j \\ j & i \end{pmatrix} \in \mathfrak{S}_n$, où $(i,j) \in [\![1,n]\!]^2$. Une telle permutation est dite* transposition.

II Orbites et cycles

II.1 Orbites

Définition 21.8 (Orbites)**.** *$s \in \mathfrak{S}_n$, $a \in [\![1,n]\!]$. On appelle* orbite de a sous l'action de s *l'ensemble $\mathscr{O}_s(a) = \{s^k(a),\ k \in \mathbb{Z}\}$.*

Proposition 21.9. *$s \in \mathfrak{S}_n$, $a \in [\![1,n]\!]$.*

(i) $\operatorname{card} \mathscr{O}_s(a) = \min\{p \in \mathbb{N}^*,\ s^p(a) = a\}$.

(ii) $(\mathscr{O}_s(\alpha))_{\alpha \in [\![1,n]\!]}$ *est une partition de $[\![1,n]\!]$.*

(iii) $\forall b \in \mathscr{O}_s(a),\ \mathscr{O}_s(a) = \mathscr{O}_s(b)$.

II.2 Cycles et composées de cycles

Définition 21.10 (Cycle)**.** *On dit que $s \in \mathfrak{S}_n$ est un* cycle *lorsque s a une seule orbite non réduite à un élément. On appelle alors cette orbite* support de s *; et on appelle* longueur de s *le cardinal du support de s.*

Vocabulaire 21.11 (Permutation circulaire)**.** *On appelle* permutation circulaire *de $\mathfrak{S}_n$ tout cycle de longueur n.*

Notation 21.12. *Soit $s \in \mathfrak{S}_n$ un cycle de longueur p et de support $\mathscr{O}_s(a) = \{a, s(a), \dots, s^{p-1}(a)\}$, où $a \in [\![1, n]\!]$. On notera $s = \big(a\, s(a) \cdots s^{p-1}(a)\big)$.*

Proposition 21.13.

(i) *Si $\sigma \in \mathfrak{S}_n$ est un cycle de longueur p, alors $\sigma^p = id$ et $\sigma^{p-1} \neq id$.*

(ii) *Soit $\sigma = (a_1\, a_2 \cdots a_p) \in \mathfrak{S}_n$, alors $\sigma^{-1} = (a_p\, a_{p-1} \cdots a_1)$.*

(iii) *Deux cycles à supports disjoints commutent.*

Théorème 21.14. *Toute permutation s'écrit de manière unique à l'ordre près comme produit de cycles à supports disjoints.*

Démonstration. *Existence.* Soit $\sigma \in \mathfrak{S}_n$. Soit k le nombre d'orbites de σ non réduites à un élément, qu'on note $\mathscr{O}_\sigma(a_1), \dots, \mathscr{O}_\sigma(a_k)$. Pour $i \in [\![1, k]\!]$, poser $\sigma_i = \Big(a_i\, \sigma(a_i) \cdots \sigma^{\ell_i - 1}(a_i)\Big)$, où $\ell_i = \operatorname{card} \mathscr{O}_\sigma(a_i)$. Montrer alors que $\sigma = \sigma_1 \cdots \sigma_k$. *Unicité.* Supposer $s_1 \cdots s_k = r_1 \cdots r_\ell \in \mathfrak{S}_n$, où $s_1, \dots, s_k$ sont des cycles à supports deux à deux disjoints dont on note $S_1, \dots, S_k$ les supports respectifs, $r_1, \dots, r_\ell$ sont des cycles à supports deux à deux disjoints dont on note $R_1, \dots, R_\ell$ les supports respectifs. Montrer que $\forall i \in [\![1, k]\!]$, $\exists! j \in [\![1, \ell]\!]$, $s_i = r_j$, d'où l'unicité. □

II.3 Permutations et transpositions

Proposition 21.15. *Tout cycle est produit (non unique) de transpositions.*

Démonstration. On a $(a_1\, a_2 \cdots a_p) = (a_1\, a_2)\,(a_2\, a_3) \cdots (a_{p-1}\, a_p)$. □

Théorème 21.16. *Toute permutation est produit (non unique) de transpositions.*

Démonstration. Par récurrence. $\mathcal{H}(n)$: Toute permutation de $\mathfrak{S}_n$ est produit de transpositions. $\mathcal{H}(2)$ est vraie. Supposer $\mathcal{H}(n)$ vraie pour $n \in [\![2, +\infty[\![$. Soit $s \in \mathfrak{S}_{n+1}$. Si $s(n+1) = n+1$, soit $\hat{s} : \left| \begin{array}{c} [\![1, n]\!] \longrightarrow [\![1, n]\!] \\ k \longmapsto s(k) \end{array} \right.$. Alors $\hat{s} \in \mathfrak{S}_n$, donc par $\mathcal{H}(n)$, $\hat{s}$ s'écrit comme produit de transpositions : $\hat{s} = \hat{\tau}_1 \cdots \hat{\tau}_\ell$. Pour $i \in [\![1, \ell]\!]$, soit $\tau_i : \left| \begin{array}{c} [\![1, n+1]\!] \longrightarrow [\![1, n+1]\!] \\ k \longmapsto \left\{ \begin{array}{l} \hat{\tau}_i(k) \text{ si } k \in [\![1, n]\!] \\ n+1 \text{ sinon} \end{array} \right. \end{array} \right.$. Alors τ_i est une transposition pour tout $i \in [\![1, \ell]\!]$ et on a $s = \tau_1 \cdots \tau_\ell$. Si $s(n+1) \neq n+1$, poser $\theta = ((n+1)\, s(n+1)) \circ s \in \mathfrak{S}_{n+1}$. On a alors $\theta(n+1) = n+1$, donc d'après le cas précédent, θ s'écrit comme produit de transpositions, donc $s = ((n+1)\, s(n+1)) \circ \theta$ aussi. Donc $\mathcal{H}(n+1)$ est vraie. □

III Signature d'une permutation

Théorème 21.17. *Il existe une unique application $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ t.q.*

(i) *Pour toute transposition $\tau \in \mathfrak{S}_n$, $\varepsilon(\tau) = -1$,*

(ii) *ε est un morphisme de groupes : $\forall (\sigma_1, \sigma_2) \in \mathfrak{S}_n^2$, $\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$.*

L'application ε est dite signature.

Démonstration. Poser

$$\varepsilon : \left| \begin{array}{l} \mathfrak{S}_n \longrightarrow \{-1, 1\} \\ \sigma \longmapsto \displaystyle\prod_{\substack{\{i,j\} \in \mathcal{P}_2(n) \\ i \neq j}} \frac{\sigma(i) - \sigma(j)}{i - j} \end{array} \right. ,$$

où $\mathcal{P}_2(n)$ est l'ensemble des parties à deux éléments de $[\![1, n]\!]$. Montrer d'abord (i), puis (ii). En déduire, grâce au théorème 21.16, que $\forall \sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma) \in \{-1, 1\}$. ε ayant une expression explicite, elle est donc bien définie. Et ε convient, et est unique (puisque ε est définie sur les transpositions, qui engendrent $\mathfrak{S}_n$). □

Corollaire 21.18.

(i) *La parité du nombre de transpositions intervenant dans la décomposition d'une permutation est indépendante de la décomposition choisie.*

(ii) *Le groupe $\mathfrak{A}_n = \operatorname{Ker} \varepsilon = \{\sigma \in \mathfrak{S}_n, \varepsilon(\sigma) = 1\}$, dit* groupe alterné, *est constitué des permutations produits d'un nombre pair de transpositions ; et on a $\operatorname{card} \mathfrak{A}_n = \frac{n!}{2}$.*

Vocabulaire 21.19 (Parité d'une permutation)**.** *Les permutations de $\mathfrak{A}_n$ sont dites* paires, *les autres* impaires.

Chapitre 22

Déterminants

I Formes n-linéaires

Définition 22.1 (Forme n-linéaire)**.** *E un $\mathbb{K}$-espace vectoriel. $f : E^n \to \mathbb{K}$ est dite* n-linéaire *lorsque pour tout $(x_1, \dots, x_{n-1}) \in E^{n-1}$ et pour tout $i \in [\![1, n]\!]$, l'application* $\left|\begin{array}{l} E \longrightarrow \mathbb{K} \\ x \longmapsto f(x_1, \dots, x_{i-1}, x, x_i, \dots, x_{n-1}) \end{array}\right.$ *est linéaire.*

Définition 22.2 (Caractère antisymétrique ou alterné)**.** *$f : E^n \to \mathbb{K}$ une forme n-linéaire.*

(i) *f est dite* antisymétrique *lorsque*

$$\forall (x_1, \dots, x_n) \in E^n,\ \forall (i,j) \in [\![1,n]\!]^2,\ i \neq j \implies f(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -f(x_1, \dots, x_j, \dots, x_i, \dots, x_n).$$

(ii) *f est dite* alternée *lorsque*

$$\forall (x_1, \dots, x_n) \in E^n,\ \Big(\exists (i,j) \in [\![1,n]\!]^2,\ i \neq j \text{ et } x_i = x_j\Big) \implies f(x_1, \dots, x_n) = 0.$$

Proposition 22.3. *$f : E^n \to \mathbb{K}$ une forme n-linéaire. f est alternée* ssi *f est antisymétrique.*

Notation 22.4. *On note $\Lambda_n(E)$ l'ensemble des formes n-linéaires alternées sur E.*

Proposition 22.5. *$(\Lambda_n(E), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.*

Proposition 22.6. *$f \in \Lambda_n(E)$, $\sigma \in \mathfrak{S}_n$, $(x_1, \dots, x_n) \in E^n$.*

$$f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right) = \varepsilon(\sigma) f(x_1, \dots, x_n). \qquad (\star)$$

Démonstration. Par récurrence. $\mathcal{H}(k)$: Si σ est le produit de k transpositions, alors $(\star)$ est vraie. □

II Déterminant d'une famille de n vecteurs d'un espace vectoriel de dimension n

Définition 22.7 (Déterminant)**.** *E un $\mathbb{K}$-espace vectoriel de dimension n. $\mathcal{B}$ une base de E. On définit*

$$\det_{\mathcal{B}} : \left| \begin{array}{c} E^n \longrightarrow \mathbb{K} \\ (x_1, \dots, x_n) \longmapsto \displaystyle\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{k=1}^{n} x_{\sigma(k),k} \end{array} \right. ,$$

où x_{ij} est la i-ième composante de x_j dans la base $\mathcal{B}$ pour $(i,j) \in [\![1,n]\!]^2$.

Théorème 22.8. *E un $\mathbb{K}$-espace vectoriel de dimension n. $\mathcal{B}$ une base de E. Alors $\det_{\mathcal{B}}$ est l'unique forme n-linéaire alternée sur E t.q. $\det_{\mathcal{B}}(\mathcal{B}) = 1$. De plus, $\Lambda_n(E) = \mathrm{Vect}(\det_{\mathcal{B}})$ et*

$$\forall f \in \Lambda_n(E),\ f = f(\mathcal{B}) \cdot \det_{\mathcal{B}}.$$

Démonstration. Soit $f \in \Lambda_n(E)$, $(x_1, \dots, x_n) \in E^n$. En notant $\mathcal{B} = (e_1, \dots, e_n)$, vérifier que

$$\begin{aligned} f(x_1, \dots, x_n) &= f\left(\sum_{i_1=1}^{n} x_{i_1,1} e_{i_1}, \dots, \sum_{i_n=1}^{n} x_{i_n,n} e_{i_n} \right) \\ &= \sum_{1 \leqslant i_1, \dots, i_n \leqslant n} \left(x_{i_1,1} \cdots x_{i_n,n} \cdot \underbrace{f(e_{i_1}, \dots, e_{i_n})}_{=0 \text{ dès que } i_k = i_\ell \text{ avec } k \neq \ell} \right) \\ &= \sum_{\sigma \in \mathfrak{S}_n} \left(x_{\sigma(1),1} \cdots x_{\sigma(n),n} \cdot f\left(e_{\sigma(1)}, \dots, e_{\sigma(n)} \right) \right) \\ &= \left(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{k=1}^{n} x_{\sigma(k),k} \right) \cdot f(e_1, \dots, e_n). \end{aligned}$$

□

III Propriétés du déterminant

III.1 Propriétés usuelles

Proposition 22.9. *E un $\mathbb{K}$-espace vectoriel de dimension n. $\mathcal{B}_1, \mathcal{B}_2$ bases de E. Alors*

$$\det_{\mathcal{B}_2} = \det_{\mathcal{B}_2}(\mathcal{B}_1) \cdot \det_{\mathcal{B}_1}.$$

Proposition 22.10. *E un $\mathbb{K}$-espace vectoriel de dimension n. $\mathcal{B}$ une base de E. Alors*

$$\forall (x_1, \dots, x_n) \in E^n,\ \det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{k=1}^{n} x_{k,\sigma(k)},$$

où x_{ij} est la i-ième composante de x_j dans la base $\mathcal{B}$ pour $(i,j) \in [\![1,n]\!]^2$.

III.2 Déterminant d'une matrice carrée

Définition 22.11 (Déterminant d'une matrice carrée)**.** *$A \in \mathbb{M}_n(\mathbb{K})$. On note $\det A$ le déterminant des n vecteurs colonnes de A dans la base canonique de $\mathbb{K}^n$.*

Notation 22.12. *On note*

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \det \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

Proposition 22.13. *$A = (a_{ij}) \in \mathbb{M}_n(\mathbb{K})$.*

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{k=1}^{n} a_{\sigma(k),k} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{k=1}^{n} a_{k,\sigma(k)}. \tag{i}$$

$$\det A = \det {}^tA. \tag{ii}$$

Corollaire 22.14. $\det I_n = 1$.

Exemple 22.15. $\begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc.$

Exemple 22.16 (Règle de Sarrus)**.**

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{12}a_{23}a_{31} + a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} - a_{21}a_{12}a_{33}$$
$$- a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11}.$$

III.3 Familles libres, matrices inversibles et déterminants

Proposition 22.17. *E un $\mathbb{K}$-espace vectoriel de dimension n. $\mathcal{B}$ une base de E, $\mathcal{F}$ une famille de n éléments de E. Alors $\mathcal{F}$ est une base de E* ssi $\det_{\mathcal{B}} \mathcal{F} \neq 0$.

Corollaire 22.18. *$A \in \mathbb{M}_n(\mathbb{K})$.*

$$A \in GL_n(\mathbb{K}) \iff \det A \neq 0.$$

IV Calculs de déterminants

IV.1 Quelques propriétés immédiates

Proposition 22.19. *$A \in \mathbb{M}_n(\mathbb{K})$, $T = (t_{ii}) \in \mathfrak{T}_n^+(\mathbb{K})$. On note $\mathfrak{C}_1, \ldots, \mathfrak{C}_n$ les n vecteurs colonnes de A.*

(i) $\forall (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$, $\det\left(\mathfrak{C}_1, \ldots, \mathfrak{C}_i + \sum_{j \neq i} \lambda_j \mathfrak{C}_j, \ldots, \mathfrak{C}_n\right) = \det A$.

(ii) $\forall \lambda \in \mathbb{K}$, $\det(\mathfrak{C}_1, \ldots, \lambda \mathfrak{C}_i, \ldots, \mathfrak{C}_n) = \lambda \det A$.

(iii) $\forall \lambda \in \mathbb{K}$, $\det(\lambda A) = \lambda^n \det A$.

(iv) $\forall \sigma \in \mathfrak{S}_n$, $\det\left(\mathfrak{C}_{\sigma(1)}, \ldots, \mathfrak{C}_{\sigma(n)}\right) = \varepsilon(\sigma) \det A$.

(v) $\det T = \prod_{i=1}^{n} t_{ii}$.

Démonstration. (v) Par récurrence. Pour $k \in [\![1, n]\!]$, poser $\mathcal{H}(k) : \det T = \left(\prod_{i=1}^{k} t_{ii}\right) \det_{\mathcal{B}}(e_1, \ldots, e_k, \mathfrak{C}_{k+1}, .$
où $\mathcal{B} = (e_1, \ldots, e_n)$ est la base canonique de $\mathbb{K}^n$. □

Remarque 22.20. *Dans la propriété précédente, les manipulations sur les colonnes peuvent aussi être effectuées sur les lignes.*

IV.2 Développement par rapport à une ligne ou une colonne.

Définition 22.21 (Mineur, cofacteur et comatrice)**.** $A \in \mathbb{M}_n(\mathbb{K})$, $(i,j) \in [\![1,n]\!]^2$.

(i) *On appelle* mineur (i,j) *de* A*, noté* M_{ij}*, le déterminant de la sous-matrice carrée de* A *d'ordre* $(n-1)$ *obtenue en retirant la* i*-ième ligne et la* j*-ième colonne de* A*.*

(ii) *On définit le* cofacteur (i,j) *de* A *par* $\operatorname{Cof}_{ij}(A) = (-1)^{i+j} M_{ij} \in \mathbb{K}$.

(iii) *On appelle* comatrice *de* A *la matrice* $\operatorname{Com} A = \sum_{1 \leqslant i,j \leqslant n} \operatorname{Cof}_{ij}(A) E_{ij} \in \mathbb{M}_n(\mathbb{K})$.

Proposition 22.22. $A = (a_{ij}) \in \mathbb{M}_n(\mathbb{K})$, $j \in [\![1,n]\!]$.

$$\det A = \sum_{i=1}^{n} a_{ij} \operatorname{Cof}_{ij}(A).$$

Remarque 22.23. *Cette propriété reste valable pour un développement par rapport à une ligne :* $\forall i \in [\![1,n]\!]$, $\det A = \sum_{j=1}^{n} a_{ij} \operatorname{Cof}_{ij}(A)$.

IV.3 Inverse d'une matrice

Proposition 22.24. $A \in \mathbb{M}_n(\mathbb{K})$*. Alors* $A \times {}^t(\operatorname{Com} A) = {}^t(\operatorname{Com} A) \times A = (\det A)\, I_n$.

V Déterminant et morphisme de groupes

V.1 Déterminant d'un endomorphisme

Proposition 22.25. E *un* $\mathbb{K}$*-espace vectoriel de dimension* n*.* $f \in \mathcal{L}(E)$.

$\exists \lambda \in \mathbb{K}$, $\forall (x_1, \ldots, x_n) \in E^n$, $\forall \mathcal{B}$ *base de* E,

$$\det_{\mathcal{B}}(f(x_1), \ldots, f(x_n)) = \lambda \det_{\mathcal{B}}(x_1, \ldots, x_n).$$

Définition 22.26 (Déterminant d'un endomorphisme)**.** E *un* $\mathbb{K}$*-espace vectoriel de dimension* n*.* $f \in \mathcal{L}(E)$*. On note* $\operatorname{Det} f$ *l'unique scalaire t.q.*

$\forall (x_1, \ldots, x_n) \in E^n$, $\forall \mathcal{B}$ *base de* E,

$$\det_{\mathcal{B}}(f(x_1), \ldots, f(x_n)) = (\operatorname{Det} f) \det_{\mathcal{B}}(x_1, \ldots, x_n).$$

Corollaire 22.27. E *un* $\mathbb{K}$*-espace vectoriel de dimension* n*.* $f \in \mathcal{L}(E)$*.* $\mathcal{B}$ *base de* E*. Alors* $\operatorname{Det} f = \det \operatorname{Mat}_{\mathcal{B}}(f)$.

Corollaire 22.28. $(A,B) \in \mathbb{M}_n(\mathbb{K})^2$*. Si* A *et* B *sont semblables alors* $\det A = \det B$.

V.2 Morphisme

Proposition 22.29. E *un* $\mathbb{K}$*-espace vectoriel de dimension* n*.* $\forall (f,g) \in \mathcal{L}(E)^2$, $\operatorname{Det}(f \circ g) = (\operatorname{Det} f)(\operatorname{Det} g)$.

Corollaire 22.30.

$$\forall (A,B) \in \mathbb{M}_n(\mathbb{K})^2,\ \det(AB) = (\det A)(\det B).$$

Proposition 22.31. E *un* $\mathbb{K}$*-espace vectoriel de dimension* n*.* $f \in \mathcal{L}(E)$, $A \in \mathbb{M}_n(\mathbb{K})$.

(i) $f \in GL(E) \iff \operatorname{Det} f \neq 0$*. Dans ce cas,* $\operatorname{Det} f^{-1} = \frac{1}{\operatorname{Det} f}$.

(ii) $A \in GL_n(\mathbb{K}) \iff \det A \neq 0$. *Dans ce cas,* $\det A^{-1} = \frac{1}{\det A}$.

(iii) *L'application* $\left|\begin{array}{c} GL(E) \longrightarrow \mathbb{K}^* \\ f \longmapsto \operatorname{Det} f \end{array}\right.$ *est un morphisme de groupes.*

Corollaire 22.32. $(A_{11}, A_{12}, A_{22}) \in \mathbb{M}_n(\mathbb{K})^3$.

$$\det \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix} = (\det A_{11})(\det A_{22}).$$

Démonstration. Écrire $\begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & A_{22} \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} \\ 0 & I_n \end{pmatrix}$. □

VI Déterminant de Vandermonde

Définition 22.33 (Déterminant de Vandermonde)**.** *Pour* $(x_0, \dots, x_n) \in \mathbb{K}^{n+1}$, *on note*

$$\mathcal{V}(x_0, \dots, x_n) = \begin{vmatrix} 1 & 1 & \cdots & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_j & \cdots & x_n \\ x_0^2 & x_1^2 & \cdots & x_j^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ x_0^i & x_1^i & \cdots & x_j^i & \cdots & x_n^i \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ x_0^n & x_1^n & \cdots & x_j^n & \cdots & x_n^n \end{vmatrix}.$$

Proposition 22.34.

$$\forall (x_0, \dots, x_n) \in \mathbb{K}^{n+1},\ \mathcal{V}(x_0, \dots, x_n) = \prod_{0 \leqslant i < j \leqslant n} (x_j - x_i). \qquad (*)$$

Démonstration. Par récurrence. $\mathcal{H}(n)$: $(*)$. $\mathcal{H}(1)$ est vraie. En supposant $\mathcal{H}(n-1)$ vraie pour $n \geqslant 2$, poser $f : x \in \mathbb{K} \longmapsto \mathcal{V}(x_0, \dots, x_{n-1}, x)$. Supposer $\forall (i,j) \in [\![0, n]\!]^2,\ i \neq j \Rightarrow x_i \neq x_j$, sinon le résultat est clair. Montrer, en développant le déterminant par rapport à la dernière colonne, que f est polynomiale de degré n et que $\forall k \in [\![0, n[\![,\ f(x_k) = 0$. Ainsi $\exists \lambda \in \mathbb{K},\ \forall x \in \mathbb{K},\ f(x) = \lambda \prod_{k=0}^{n-1} (x - x_k)$. Montrer que $\lambda = \mathcal{V}(x_0, \dots, x_{n-1})$ et en déduire $\mathcal{H}(n)$. □

Chapitre 23

Résolution de Systèmes Linéaires

I Notion de sous-espace affine

Définition 23.1 (Sous-espace affine)**.** *E un $\mathbb{K}$-espace vectoriel. $M_0 \in E$, F un sous-espace vectoriel de E. On appelle* sous-espace affine *de E passant par M_0 et de direction F l'ensemble*

$$\mathscr{F} = M_0 + F = \{M_0 + u,\ u \in F\}.$$

Les éléments de $\mathscr{F}$ sont dits points *de $\mathscr{F}$.*

Notation 23.2. *E un $\mathbb{K}$-espace vectoriel. $\mathscr{F} = M_0 + F$ un sous-espace affine de E, où $M_0 \in E$, F sous-espace vectoriel de E. Pour $M \in \mathscr{F}$, on note $\overrightarrow{M_0M} = M - M_0 \in F$.*

Définition 23.3 (Dimension d'un sous-espace affine)**.** *E un $\mathbb{K}$-espace vectoriel. $\mathscr{F}$ un sous-espace affine de E de direction F. On dit que $\mathscr{F}$ est de dimension finie lorsque F est de dimension finie et on définit alors* $\dim \mathscr{F} = \dim F$.

Lemme 23.4. *E un $\mathbb{K}$-espace vectoriel. $\mathscr{F}$ un sous-espace affine de E de direction F. Alors $\forall M \in \mathscr{F}$, $\mathscr{F} = M + F$.*

Proposition 23.5. *E un $\mathbb{K}$-espace vectoriel. $\mathscr{F}$ et $\mathscr{G}$ deux sous-espaces affines de E de directions respectives F et G. Alors $\mathscr{F} \cap \mathscr{G}$ est soit vide, soit un sous-espace affine de E de direction $F \cap G$.*

II Application aux systèmes linéaires

Proposition 23.6. *$A \in \mathbb{M}_{n,p}(\mathbb{K})$, $B \in \mathbb{M}_{n,1}(\mathbb{K})$. Alors l'ensemble $\mathscr{S}$, défini par $\mathscr{S} = \{X \in \mathbb{K}^p,\ AX = B\}$, est soit vide, soit un sous-espace affine de $\mathbb{K}^p$ de direction* $\operatorname{Ker} A$. *Autrement dit, $\mathscr{S}$ est l'intersection de n hyperplans affines de $\mathbb{K}^p$.*

Définition 23.7 (Rang d'un système linéaire)**.** *$A \in \mathbb{M}_{n,p}(\mathbb{K})$, $B \in \mathbb{M}_{n,1}(\mathbb{K})$. On appelle rang du système $AX = B$ le rang de A.*

Proposition 23.8. *$A \in \mathbb{M}_{n,p}(\mathbb{K})$, $B \in \mathbb{M}_{n,1}(\mathbb{K})$. $\mathscr{S} = \{X \in \mathbb{K}^p,\ AX = B\}$. Si $\operatorname{rg} A = n$ alors $\mathscr{S} \neq \varnothing$. Si $\operatorname{rg} A < n$ alors $\mathscr{S} \neq \varnothing$* ssi *$B \in \operatorname{Im} A$. Dans ce cas, B appartient à l'intersection de $(n - \operatorname{rg} A)$ hyperplans ; on dit que B doit satisfaire à $(n - \operatorname{rg} A)$* relations de compatibilité.

Corollaire 23.9. *$A \in \mathbb{M}_n(\mathbb{K})$, $B \in \mathbb{M}_{n,1}(\mathbb{K})$. Alors le système $AX = B$ a une unique solution* ssi *$A \in GL_n(\mathbb{K})$. Dans ce cas, le système est dit* système de Cramer.

III Méthode de Gauss

Proposition 23.10. *$T \in \mathfrak{T}_n^+(\mathbb{K}) \cap GL_n(\mathbb{K})$. $B \in \mathbb{M}_{n,1}(\mathbb{K})$. Alors la résolution du système $TX = B$ s'effectue en un nombre d'opérations équivalent à n^2 (ou $\frac{n^2}{2}$ si on ne compte pas les additions).*

Méthode 23.11 (Méthode de Gauss)**.** *$A = (a_{ij}) \in \mathbb{M}_{n,p}(\mathbb{K}) \setminus \{0\}$, $B \in \mathbb{M}_{n,1}(\mathbb{K})$. On cherche à résoudre le système linéaire $AX = B$.*

(i) *Si la première colonne est nulle, alors on permute deux colonnes pour se ramener à une première colonne non nulle. Si $a_{11} = 0$, alors on permute deux lignes pour se ramener au cas $a_{11} \neq 0$. On effectue ensuite des opérations de transvection afin que tous les coefficients de la première colonne soient nuls sauf a_{11}.*

(ii) *On réitère l'étape* (i) *jusqu'à ce que la sous-matrice constituée des $(n-k)$ dernières lignes et $(p-k)$ dernières colonnes de A soit nulle. On se ramène ainsi à la résolution d'un système triangulaire.*

Cette méthode permet de résoudre $AX = B$ en un nombre d'opérations équivalent à $\frac{2n^3}{3}$ (ou $\frac{n^3}{3}$ si on ne compte pas les additions).

Chapitre 24

Intégration sur un Segment

I Uniforme continuité

Définition 24.1 (Uniforme continuité)**.** $f : I \to \mathbb{R}$. *On dit que* f *est* uniformément continue *(*$\mathcal{UC}^0$*) sur* I *lorsque*

$$\forall \varepsilon > 0,\ \exists \eta \in \mathbb{R}_+^*,\ \forall (x,y) \in I^2,\ |x-y| < \eta \Longrightarrow |f(x) - f(y)| < \varepsilon.$$

Proposition 24.2.

(i) *Toute fonction lipschitzienne sur* I *est uniformément continue sur* I*.*

(ii) *Toute fonction uniformément continue sur* I *est continue sur* I*.*

Proposition 24.3. $f : I \to \mathbb{R}$. f *est non* $\mathcal{UC}^0$ *sur* I ssi *il existe* $(a_n) \in I^{\mathbb{N}}$, $(b_n) \in I^{\mathbb{N}}$ *et* $\varepsilon > 0$ *t.q.* $(a_n - b_n) \xrightarrow[n\to+\infty]{} 0$ *mais* $\forall n \in \mathbb{N}$, $|f(a_n) - f(b_n)| \geqslant \varepsilon$.

Théorème 24.4 (Théorème de Heine)**.** *Toute fonction à valeurs réelles* $\mathcal{C}^0$ *sur un segment* $[a,b]$ *est* $\mathcal{UC}^0$ *sur* $[a,b]$*.*

Démonstration. $f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0$. Supposer par l'absurde f non $\mathcal{UC}^0$. Alors il existe $(\alpha_n) \in [a,b]^{\mathbb{N}}$, $(\beta_n) \in [a,b]^{\mathbb{N}}$ et $\varepsilon > 0$ t.q. $(\alpha_n - \beta_n) \xrightarrow[n\to+\infty]{} 0$ et $\forall n \in \mathbb{N}$, $|f(\alpha_n) - f(\beta_n)| \geqslant \varepsilon$. Comme (α_n) est bornée, en extraire une sous-suite convergente $\left(\alpha_{\varphi(n)}\right)$ (avec $\varphi : \mathbb{N} \to \mathbb{N} \nearrow\nearrow$) t.q. $\alpha_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell \in [a,b]$. De plus, $\left(\alpha_{\varphi(n)} - \beta_{\varphi(n)}\right) \xrightarrow[n\to+\infty]{} 0$, d'où $\beta_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell$. Mais f est $\mathcal{C}^0$ sur $[a,b]$ et $\ell \in [a,b]$ donc $f\left(\alpha_{\varphi(n)}\right) \xrightarrow[n\to+\infty]{} f(\ell)$ et $f\left(\beta_{\varphi(n)}\right) \xrightarrow[n\to+\infty]{} f(\ell)$, donc $\left|f\left(\alpha_{\varphi(n)}\right) - f\left(\beta_{\varphi(n)}\right)\right| \xrightarrow[n\to+\infty]{} 0$. C'est une contradiction. □

II Fonctions en escaliers et fonctions continues par morceaux

II.1 Subdivisions

Définition 24.5 (Subdivisions)**.** $(a,b) \in \mathbb{R}^2$, $a < b$. *On appelle* subdivision *de* $[a,b]$ *toute suite finie* $\sigma = (a_0, \ldots, a_n)$ *avec* $a = a_0 < a_1 < \cdots < a_n = b$.

(i) *On appelle* support *de* σ *l'ensemble* $\mathcal{S}_\sigma = \{a_0, \ldots, a_n\}$.

(ii) *On appelle* pas *de* σ *le réel* $\max_{i \in [\![0,n[\![} |a_{i+1} - a_i|$.

On appelle de plus subdivision régulière *de* $[a,b]$ *de pas* h *la subdivision* $(a, a+h, \dots, a+nh)$ *avec* $h = \frac{b-a}{n}$.

Vocabulaire 24.6. *σ_1 et σ_2 deux subdivisions de $[a,b]$. On dit que σ_2 est plus fine que σ_1 lorsque $\mathcal{S}_{\sigma_1} \subset \mathcal{S}_{\sigma_2}$.*

Notation 24.7. *σ_1 et σ_2 deux subdivisions de $[a,b]$. On note $\sigma_1 \cup \sigma_2$ la subdivision de $[a,b]$ de support $\mathcal{S}_{\sigma_1} \cup \mathcal{S}_{\sigma_2}$.*

II.2 Fonctions en escaliers

Définition 24.8 (Fonctions en escaliers)**.** *$f : [a,b] \to \mathbb{R}$. f est dite* en escaliers *sur $[a,b]$ lorsqu'il existe une subdivision $\sigma = (a_0, \dots, a_n)$ de $[a,b]$ t.q. $\forall i \in [\![0,n[\![$, $f_{]a_i,a_{i+1}[}$ est constante. σ est alors dite* subdivision adaptée *à f.*

Notation 24.9. *$f : [a,b] \to \mathbb{R}$ en escaliers, $\sigma = (a_0, \dots, a_n)$ subdivision adaptée à f. On écrit*

$$f = \sum_{i=0}^{n-1} \lambda_i \mathbb{1}_{]a_i,a_{i+1}[} \quad \text{sur } [a,b] \backslash \mathcal{S}_\sigma,$$

où, pour $i \in [\![0,n[\![$, λ_i est la constante t.q. $f_{]a_i,a_{i+1}[} = \lambda_i$.

Notation 24.10. *On note $\mathcal{E}_{[a,b]}$ l'ensemble des fonctions en escaliers sur $[a,b]$ à valeurs dans $\mathbb{R}$.*

Proposition 24.11.

(i) *Toute subdivision plus fine d'une subdivision adaptée à une fonction f en escaliers sur $[a,b]$ est aussi adaptée à f.*

(ii) *L'ensemble $\mathcal{E}_{[a,b]}$ des fonctions en escaliers sur $[a,b]$ à valeurs dans $\mathbb{R}$ est un espace vectoriel stable par produit et inclus dans l'ensemble des fonctions bornées sur $[a,b]$.*

II.3 Fonctions continues par morceaux

Définition 24.12 (Fonctions continues par morceaux)**.** *$f : [a,b] \to \mathbb{R}$. f est dite* continue par morceaux *($\mathcal{C}^0_{pm}$) sur $[a,b]$ lorsqu'il existe une subdivision $\sigma = (a_0, \dots, a_n)$ de $[a,b]$ t.q. $\forall i \in [\![0,n[\![$, $f_{]a_i,a_{i+1}[}$ est $\mathcal{C}^0$ et, pour tout $i \in [\![0,n]\!]$, f admet une limite réelle à droite et à gauche en a_i. σ est alors dite* subdivision adaptée *à f.*

Proposition 24.13. *$f : [a,b] \to \mathbb{R}$. f est continue par morceaux* ssi *il existe une subdivision $(a_0, \dots, a_n)$ de $[a,b]$ et des fonctions $f_i : [a_i, a_{i+1}] \to \mathbb{R}$ $\mathcal{C}^0$ pour $i \in [\![0,n[\![$ t.q. $\forall i \in [\![0,n[\![$, $f_{]a_i,a_{i+1}[} = f_{i\,]a_i,a_{i+1}[}$*

Notation 24.14. *On note $\mathcal{C}^0_{pm}([a,b], \mathbb{R})$ l'ensemble des fonctions $\mathcal{C}^0_{pm}$ sur $[a,b]$ à valeurs dans $\mathbb{R}$.*

Proposition 24.15.

(i) *Toute subdivision plus fine d'une subdivision adaptée à une fonction f $\mathcal{C}^0_{pm}$ sur $[a,b]$ est aussi adaptée à f.*

(ii) *L'ensemble $\mathcal{C}^0_{pm}([a,b], \mathbb{R})$ des fonctions $\mathcal{C}^0_{pm}$ sur $[a,b]$ à valeurs dans $\mathbb{R}$ est un espace vectoriel stable par produit et inclus dans l'ensemble des fonctions bornées sur $[a,b]$.*

Proposition 24.16. *$f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0_{pm}$. $\varphi : [c,d] \to \mathbb{R}$ avec $\varphi([c,d]) \subset [a,b]$. Si φ est $\mathcal{C}^0$ et strictement monotone sur $[c,d]$, alors $(f \circ \varphi)$ est $\mathcal{C}^0_{pm}$ sur J.*

Démonstration. Supposer $\varphi \nearrow\nearrow$. Soit $(a_0, \dots, a_n)$ une subdivision adaptée à f. Poser $\alpha_i = \varphi^{-1}(a_i)$ pour $i \in [\![0,n]\!]$ (par bijectivité de φ). Montrer alors que $(f \circ \varphi)$ est $\mathcal{C}^0_{pm}$, $(\alpha_0, \dots, \alpha_n)$ étant une subdivision adaptée à $(f \circ \varphi)$. □

II.4 Approximation de fonctions continues par morceaux

Notation 24.17. *On définit sur l'ensemble des fonctions bornées $I \to \mathbb{R}$ la norme $\|\cdot\|_I^\infty$ par*

$$\forall \varphi \in \mathbb{R}^I \text{ bornée, } \|\varphi\|_I^\infty = \sup_I |\varphi|.$$

Définition 24.18 (Convergence uniforme)**.** *(f_n) une suite de fonctions $I \to \mathbb{R}$, $f : I \to \mathbb{R}$. On dit que (f_n)* converge uniformément *vers f sur I lorsque*

$$\|f_n - f\|_I^\infty \xrightarrow[n\to+\infty]{} 0.$$

Définition 24.19 (Convergence simple)**.** *(f_n) une suite de fonctions $I \to \mathbb{R}$, $f : I \to \mathbb{R}$. On dit que (f_n)* converge simplement *vers f sur I lorsque*

$$\forall x \in I,\ |f_n(x) - f(x)| \xrightarrow[n\to+\infty]{} 0.$$

Proposition 24.20. *(f_n) une suite de fonctions $I \to \mathbb{R}$, $f : I \to \mathbb{R}$. Si (f_n) converge uniformément vers f sur I alors (f_n) converge simplement vers f sur I.*

Théorème 24.21. *Toute fonction $\mathcal{C}^0_{pm}$ sur un segment $[a,b]$ est limite uniforme d'une suite de fonctions en escaliers sur $[a,b]$.*

Démonstration. $f : [a,b] \to \mathbb{R}$. *Première étape.* Supposer f $\mathcal{C}^0$. Pour $n \in \mathbb{N}^*$, introduire la subdivision régulière $(a, a+h, \dots, a+nh)$ avec $h = \frac{b-a}{n}$, et poser $f_n : x \in [a,b] \longmapsto \begin{cases} f(a_k) & \text{si } x \in [a_k, a_{k+1}[\text{ pour } k \in [\![0,n[\![\\ f(b) & \text{si } x = b \end{cases}$ (f_n est en escaliers). Soit $\varepsilon > 0$. Comme, f est $\mathcal{C}^0$ sur $[a,b]$ donc $\mathcal{UC}^0$ sur $[a,b]$, $\exists \eta \in \mathbb{R}_+^*$, $\forall (x,y) \in [a,b]^2$, $|x-y| < \eta \implies |f(x) - f(y)| < \varepsilon$. Soit $n > \frac{b-a}{\eta}$, alors $\forall k \in [\![0,n[\![$, $\forall x \in [a_k, a_{k+1}[$, $|x - a_k| < \eta$ donc $\forall k \in [\![0,n[\![$, $\forall x \in [a_k, a_{k+1}[$, $|f(x) - f_n(x)| = |f(x) - f(a_k)| < \varepsilon$, et c'est encore vrai en $x = b$. Donc $\sup_{[a,b]} |f - f_n| < \varepsilon$. Donc (f_n) converge uniformément vers f. *Deuxième étape.* Supposer f $\mathcal{C}^0_{pm}$. Soit $(\alpha_0, \dots, \alpha_p)$ une subdivision de $[a,b]$ adaptée à f. Pour $i \in [\![0,p[\![$, soit $f_i : [\alpha_i, \alpha_{i+1}] \to \mathbb{R}$ $\mathcal{C}^0$ t.q. $f_{i|]\alpha_i,\alpha_{i+1}[} = f_{|]\alpha_i,\alpha_{i+1}[}$, et soit $(f_{i,n})$ une suite de fonctions en escaliers définies sur $]\alpha_i, \alpha_{i+1}[$ convergeant uniformément vers f_i (qui existe d'après la première étape). Poser alors, pour $n \in \mathbb{N}$, $\varphi_n : x \in [a,b] \longmapsto \begin{cases} f_{i,n}(x) & \text{si } x \in]\alpha_i, \alpha_{i+1}[\text{ pour } i \in [\![0,p[\![\\ f(\alpha_i) & \text{si } x = \alpha_i \text{ pour } i \in [\![0,p]\!] \end{cases}$. Vérifier alors que (φ_n) est une suite de fonctions en escaliers convergeant uniformément vers f sur $[a,b]$. □

III Intégrales de fonctions en escaliers sur un segment

Définition 24.22 (Intégrale d'une fonction en escaliers)**.** *$\varphi \in \mathcal{E}_{[a,b]}$, $\sigma = (a_0, \dots, a_n)$ une subdivision adaptée à φ. On définit*

$$\int_a^b \varphi = \sum_{k=0}^{n-1} (a_{k+1} - a_k)\, \varphi(c_k),$$

où $c_k \in]a_k, a_{k+1}[$ pour $k \in [\![0,n[\![$.

Démonstration. Il faut justifier que $\int_a^b \varphi$, que l'on note pour l'instant $I_\sigma(\varphi)$, est indépendante de la subdivision σ choisie. Montrer pour cela que si $\hat{\sigma}$ est une subdivision plus fine que σ, alors $I_\sigma(\varphi) = I_{\hat{\sigma}}(\varphi)$. Montrer alors que pour toute autre subdivision σ' adaptée à φ, on a $I_\sigma(\varphi) = I_{\sigma \cup \sigma'}(\varphi) = I_{\sigma'}(\varphi)$. □

Proposition 24.23. *$\varphi \in \mathcal{E}_{[a,b]}$. Alors $\int_a^b \varphi$ n'est pas modifiée lorsque la valeur de φ est modifiée en un nombre fini de points de $[a,b]$.*

Proposition 24.24.

(i) *L'application* $\left|\begin{array}{l}\mathcal{E}_{[a,b]} \longrightarrow \mathbb{R} \\ \quad \varphi \longmapsto \displaystyle\int_a^b \varphi\end{array}\right.$ *est une forme linéaire.*

(ii) $\forall \varphi \in \mathcal{E}_{[a,b]},\ \varphi \geqslant 0$ *sur* $[a,b] \Longrightarrow \int_a^b \varphi \geqslant 0$.

(iii) $\forall (\varphi,\psi) \in \mathcal{E}_{[a,b]}^2,\ \varphi \geqslant \psi$ *sur* $[a,b] \Longrightarrow \int_a^b \varphi \geqslant \int_a^b \psi$.

(iv) $\forall \varphi \in \mathcal{E}_{[a,b]},\ |\varphi| \in \mathcal{E}_{[a,b]}$ *et*

$$\left|\int_a^b \varphi\right| \leqslant \int_a^b |\varphi|\,.$$

(v) $\forall \varphi \in \mathbb{R}^{[a,b]},\ \forall c \in]a,b[,\ \varphi \in \mathcal{E}_{[a,b]} \Longleftrightarrow \varphi_{|[a,c]} \in \mathcal{E}_{[a,c]}$ et $\varphi_{|[c,b]} \in \mathcal{E}_{[c,b]}$ *et dans ce cas*

$$\int_a^b \varphi = \int_a^c \varphi + \int_c^b \varphi.$$

Proposition 24.25. *$\varphi \in \mathcal{E}_{[a,b]}$.*

$$\left|\int_a^b \varphi\right| \leqslant (b-a)\,\|\varphi\|_{[a,b]}^{\infty}\,.$$

Proposition 24.26 (Changement de variable affine)**.** *$\varphi \in \mathcal{E}_{[a,b]}$. $\lambda \in \mathbb{R}_+^*, \mu \in \mathbb{R}$.*

$$\int_a^b \varphi(x)\ \mathrm{d}x = \lambda \int_{\frac{a-\mu}{\lambda}}^{\frac{b-\mu}{\lambda}} \varphi(\lambda t + \mu)\ \mathrm{d}t.$$

IV Intégrales de fonctions continues par morceaux sur un segment

Définition 24.27 (Riemann-intégrabilité)**.** *$f : [a,b] \to \mathbb{R}$ bornée. On note $\mathcal{E}^- = \left\{\varphi \in \mathcal{E}_{[a,b]},\ \varphi \leqslant f \text{ sur } [a,b]\right\}$ et $\mathcal{E}^+ = \left\{\psi \in \mathcal{E}_{[a,b]},\ \psi \geqslant f \text{ sur } [a,b]\right\}$, et*

$$I^- = \sup_{\varphi \in \mathcal{E}^-} \int_a^b \varphi \qquad \text{et} \qquad I^+ = \inf_{\psi \in \mathcal{E}^+} \int_a^b \psi.$$

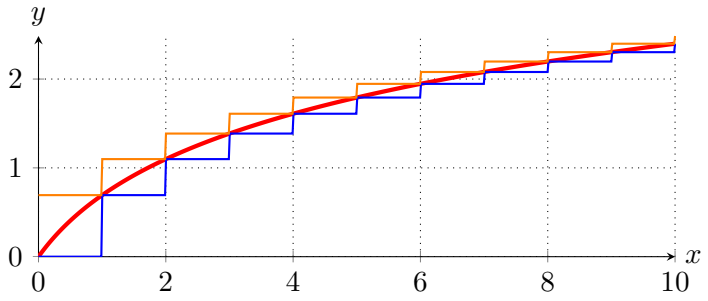
On dit que f est Riemann-intégrable *sur $[a,b]$ lorsque $I^+ = I^-$, et on note alors $\int_a^b f = I^+ = I^-$.*

Lemme 24.28. *Si f est $\mathcal{C}_{pm}^0$ sur $[a,b]$, alors*

$$\forall \varepsilon > 0,\ \exists (\varphi,\psi) \in \mathcal{E}_{[a,b]}^2,\ \varphi \leqslant f \leqslant \psi \text{ et } 0 \leqslant \psi - \varphi \leqslant \varepsilon.$$

Démonstration. Conséquence du théorème 24.21. □

Proposition 24.29. *Toute fonction $\mathcal{C}_{pm}^0$ sur $[a,b]$ est Riemann-intégrable sur $[a,b]$.*



Approximation d'une fonction continue par des fonctions en escaliers

Démonstration. Soit $f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0_{pm}$. Montrer d'abord (avec les notations de la définition 24.27) que $I^- \leqslant I^+$. Montrer ensuite que $\forall \varepsilon > 0$, $I^+ - I^- \leqslant \varepsilon(b-a)$ (en utilisant le lemme 24.28), et en déduire que $I^+ = I^-$. □

Proposition 24.30. *$f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0_{pm}$, (φ_n) une suite de fonctions en escaliers convergeant uniformément vers f. Alors*

$$\int_a^b \varphi_n \xrightarrow[n\to+\infty]{} \int_a^b f.$$

Théorème 24.31 (Sommes de Riemann)**.** *$f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0_{pm}$. Pour $n \in \mathbb{N}^*$, on pose*

$$\mathcal{S}_n(f) = \frac{b-a}{n} \sum_{k=0}^{n-1} f(a_k),$$

où $a_k = a + k\frac{b-a}{n}$ pour $k \in [\![0,n]\!]$. Alors

$$\mathcal{S}_n(f) \xrightarrow[n\to+\infty]{} \int_a^b f.$$

Démonstration. Construire une suite (φ_n) de fonctions en escaliers sur $[a,b]$ convergeant uniformément vers f sur $[a,b]$ comme dans la démonstration du théorème 24.21. En déduire que $\mathcal{S}_n(f) = \int_a^b \varphi_n \xrightarrow[n\to+\infty]{} \int_a^b f$. □

V Propriétés de l'intégrale

V.1 Propriétés obtenues par densité

Proposition 24.32. *$f \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})$. Alors $\int_a^b f$ n'est pas modifiée lorsque la valeur de f est modifiée en un nombre fini de points de $[a,b]$.*

Proposition 24.33.

(i) *L'application* $\left|\begin{array}{ccc} \mathcal{C}^0_{pm}([a,b],\mathbb{R}) & \longrightarrow & \mathbb{R} \\ f & \longmapsto & \displaystyle\int_a^b f \end{array}\right.$ *est une forme linéaire.*

(ii) $\forall f \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})$, $f \geqslant 0$ *sur* $[a,b] \Longrightarrow \int_a^b f \geqslant 0$.

(iii) $\forall (f,g) \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})^2$, $f \geqslant g$ *sur* $[a,b] \Longrightarrow \int_a^b f \geqslant \int_a^b g$.

(iv) $\forall f \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})$, $|f| \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})$ *et*

$$\left|\int_a^b f\right| \leqslant \int_a^b |f|.$$

(v) $\forall f \in \mathbb{R}^{[a,b]}$, $\forall c \in]a,b[$, $f \in \mathcal{C}^0_{pm}([a,b],\mathbb{R}) \iff f_{|[a,c]} \in \mathcal{C}^0_{pm}([a,c],\mathbb{R})$ et $f_{|[c,b]} \in \mathcal{C}^0_{pm}([c,b],\mathbb{R})$ *et dans ce cas*

$$\int_a^b f = \int_a^c f + \int_c^b f.$$

Proposition 24.34 (Changement de variable affine)**.** $f \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})$. $\lambda \in \mathbb{R}_+^*, \mu \in \mathbb{R}$.

$$\int_a^b f(x)\,\mathrm{d}x = \lambda \int_{\frac{a-\mu}{\lambda}}^{\frac{b-\mu}{\lambda}} f(\lambda t+\mu)\,\mathrm{d}t.$$

Corollaire 24.35. $f : \mathbb{R} \to \mathbb{R}$ $\mathcal{C}^0_{pm}$ *sur* $[0,T]$ *et* T*-périodique* ($T > 0$)*. Alors*

$$\forall a \in \mathbb{R},\ \int_a^{a+T} f = \int_0^T f.$$

V.2 Inégalités et intégrales

Proposition 24.36 (Inégalité de la moyenne)**.** $(f,g) \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})^2$.

$$\int_a^b |f| \leqslant (b-a)\,\|f\|_{\infty,[a,b]}. \tag{i}$$

$$\left|\int_a^b fg\right| \leqslant \|f\|_{\infty,[a,b]} \int_a^b |g|. \tag{ii}$$

Corollaire 24.37. $f \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})$, (f_n) *une suite de fonctions* $\mathcal{C}^0_{pm}$ *convergeant uniformément vers* f*. Alors*

$$\int_a^b f_n \xrightarrow[n\to+\infty]{} \int_a^b f.$$

Proposition 24.38 (Inégalité de Cauchy-Schwarz)**.** $(f,g) \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})^2$.

$$\left|\int_a^b fg\right| \leqslant \sqrt{\int_a^b f^2}\sqrt{\int_a^b g^2}.$$

Démonstration. Considérer la fonction $\vartheta : \lambda \in \mathbb{R} \longmapsto \int_a^b (\lambda f+g)^2$. Montrer que $\vartheta \in \mathbb{R}_2[X]$, que $\vartheta \geqslant 0$ sur $\mathbb{R}$. En déduire que le discriminant de ϑ est négatif (si $\deg\vartheta = 2$) ou que ϑ est constante (si $\deg\vartheta < 2$). □

Corollaire 24.39 (Inégalité de Minkowski)**.** *On pose*

$$\mathfrak{N} : f \in \mathcal{C}^0_{pm}([a,b],\mathbb{R}) \longmapsto \sqrt{\int_a^b f^2}.$$

Alors

$$\forall (f,g) \in \mathcal{C}^0_{pm}([a,b],\mathbb{R})^2,\ \mathfrak{N}(f+g) \leqslant \mathfrak{N}(f) + \mathfrak{N}(g).$$

V.3 Cas d'égalité

Proposition 24.40. $f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0$.

$$\left.\begin{array}{r} f \geqslant 0 \text{ sur } [a,b] \\ \int_a^b f = 0 \end{array}\right\} \Longrightarrow f = 0 \text{ sur } [a,b].$$

Proposition 24.41. *$f, g : [a,b] \to \mathbb{R}$ $\mathcal{C}^0$. Les cas d'égalité dans les inégalités de Cauchy-Schwarz (proposition 24.38) et de Minkowski (corollaire 24.39) sont vérifiés* ssi *f et g sont colinéaires.*

Proposition 24.42 (Égalité de la moyenne)**.** *$f, g : [a,b] \to \mathbb{R}$ $\mathcal{C}^0$.*

$$g \geqslant 0 \text{ sur } [a,b] \Longrightarrow \exists c \in [a,b],\ \int_a^b fg = f(c) \int_a^b g.$$

Démonstration. Supposer $g \neq 0$ (sinon le résultat est clair). Utiliser le fait que f est bornée et atteint ses bornes sur $[a,b]$ (car f $\mathcal{C}^0$) : en notant $m = \min_{[a,b]} f$, $M = \max_{[a,b]} f$, on a $m \leqslant \frac{\int_a^b fg}{\int_a^b g} \leqslant M$. Comme m et M sont atteints par f, le TVI assure alors l'existence de c. □

VI Intégrales de fonctions à valeurs complexes

Définition 24.43 (Intégrale d'une fonction à valeurs complexes)**.** *$f : [a,b] \to \mathbb{C}$. f est dite $\mathcal{C}^0_{pm}$ sur $[a,b]$ lorsque $\Re(f)$ et $\Im(f)$ le sont. Dans ce cas, on définit*

$$\int_a^b f = \int_a^b \Re(f) + i \int_a^b \Im(f).$$

Notation 24.44. *$f \in \mathcal{C}^0_{pm}([a,b], \mathbb{C})$. K un segment inclus dans $[a,b]$. On pose :*

$$\int_b^a f = -\int_a^b f \qquad \text{et} \qquad \int_a^a f = 0 \qquad \text{et} \qquad \int_K f = \int_{\inf K}^{\sup K} f.$$

Proposition 24.45. *$f \in \mathcal{C}^0_{pm}([a,b], \mathbb{C})$. Alors*

$$\left| \int_a^b f \right| \leqslant \int_a^b |f|.$$

Démonstration. Soit θ un argument de $\int_a^b f$. On a :

$$\begin{aligned} \left| \int_a^b f \right| &= e^{-i\theta} \int_a^b f = \int_a^b f \cdot e^{-i\theta} \\ &= \Re\left(\int_a^b f \cdot e^{-i\theta} \right) = \int_a^b \Re\left(f \cdot e^{-i\theta} \right) \\ &\leqslant \int_a^b \left| f \cdot e^{-i\theta} \right| = \int_a^b |f|. \end{aligned}$$

□

Proposition 24.46 (Inégalité de Cauchy-Schwarz)**.** $(f,g) \in \mathcal{C}^0_{pm}([a,b],\mathbb{C})^2$.

$$\left|\int_a^b f\overline{g}\right| \leqslant \sqrt{\int_a^b |f|^2}\sqrt{\int_a^b |g|^2}.$$

Corollaire 24.47 (Inégalité de Minkowski)**.** *On pose*

$$\mathfrak{N} : f \in \mathcal{C}^0_{pm}([a,b],\mathbb{C}) \longmapsto \sqrt{\int_a^b |f|^2}.$$

Alors

$$\forall (f,g) \in \mathcal{C}^0_{pm}([a,b],\mathbb{C})^2,\ \mathfrak{N}(f+g) \leqslant \mathfrak{N}(f) + \mathfrak{N}(g).$$

VII Primitives et conséquences

Théorème 24.48. *$f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0$. Alors la fonction*

$$F : x \in [a,b] \longmapsto \int_a^x f$$

est $\mathcal{C}^1$ sur $[a,b]$ et vérifie $F' = f$.

Proposition 24.49 (Intégration par parties)**.** *$u, v : [a,b] \to \mathbb{R}$ $\mathcal{C}^1$. Alors*

$$\int_a^b u'v = [uv]_a^b - \int_a^b uv'.$$

Proposition 24.50 (Intégration par substitution)**.** *$f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0$. $\varphi : [c,d] \to \mathbb{R}$ $\mathcal{C}^1$ avec $\varphi([c,d]) \subset [a,b]$.*

$$\int_{\varphi(c)}^{\varphi(d)} f = \int_c^d (f \circ \varphi)\varphi'.$$

Chapitre 25

Séries

I Généralités

Définition 25.1 (Série)**.** *Soit* $(u_n) \in \mathbb{K}^{\mathbb{N}}$*. On appelle* suite des sommes partielles *associées à* (u_n) *la suite de terme général* $S_n = \sum_{k=0}^{n} u_k$*. Étudier la* série *de terme général* u_n*, notée* $\sum u_n$*, c'est étudier la nature de la suite* (S_n)*.*

(i) *On dit que* $\sum u_n$ converge *lorsque* (S_n) *converge. Dans ce cas, on appelle* somme de la série *la limite des sommes partielles :*

$$\sum_{k=0}^{\infty} u_k = \lim_{n\to+\infty} \sum_{k=0}^{n} u_k.$$

(ii) *On dit que* $\sum u_n$ diverge *lorsque* (S_n) *diverge.*

Proposition 25.2. $(u_n) \in \mathbb{K}^{\mathbb{N}}$*,* $n_0 \in \mathbb{N}$*. Alors la série associée à* $(u_n)_{n\geqslant 0}$ *converge* ssi *la série associée à* $(u_n)_{n\geqslant n_0}$ *converge. Et dans ce cas :*

$$\sum_{k=0}^{\infty} u_k = \sum_{k=0}^{n_0-1} u_k + \sum_{k=n_0}^{\infty} u_k.$$

Proposition 25.3. $(u_n) \in \mathbb{K}^{\mathbb{N}}$*,* (S_n) *la suite des sommes partielles associées à* (u_n)*. Alors* $\forall n \in \mathbb{N},\ u_{n+1} = S_{n+1} - S_n$*.*

Corollaire 25.4. $(u_n) \in \mathbb{K}^{\mathbb{N}}$*. Si* $\sum u_n$ *converge, alors* $u_n \xrightarrow[n\to+\infty]{} 0$*.*

Vocabulaire 25.5 (Divergence grossière)**.** $(u_n) \in \mathbb{K}^{\mathbb{N}}$*. On dit que* $\sum u_n$ diverge grossièrement *lorsque* (u_n) *ne tend pas vers* 0*.*

Proposition 25.6. *L'ensemble* $\left\{(u_n) \in \mathbb{K}^{\mathbb{N}},\ \sum u_n \text{ converge}\right\}$ *est un* $\mathbb{K}$*-espace vectoriel.*

II Séries à termes réels

II.1 Séries à termes positifs

Proposition 25.7. $(u_n) \in (\mathbb{R}_+)^{\mathbb{N}}$*,* (S_n) *la suite des sommes partielles associées à* (u_n)*.*

(i) (S_n) *est croissante.*

(ii) $\sum u_n$ *converge* ssi (S_n) *est majorée.*

Proposition 25.8. $(u_n) \in \mathbb{R}^{\mathbb{N}}$, $(v_n) \in \mathbb{R}^{\mathbb{N}}$. *On suppose que* $0 \leqslant u_n \leqslant v_n$ *à PCR.*

(i) $\sum v_n$ *converge* $\Longrightarrow \sum u_n$ *converge.*

(ii) $\sum u_n$ *diverge* $\Longrightarrow \sum v_n$ *diverge.*

Proposition 25.9. $(u_n) \in \mathbb{R}^{\mathbb{N}}$, $(v_n) \in \mathbb{R}^{\mathbb{N}}$ *t.q.* $u_n \geqslant 0$ *et* $v_n \geqslant 0$ *à PCR.*

(i) *Si* $u_n = \mathcal{O}(v_n)$ *et* $\sum v_n$ *converge alors* $\sum u_n$ *converge. Dans ce cas*

$$\sum_{k=n}^{\infty} u_k = \mathcal{O}\left(\sum_{k=n}^{\infty} v_k\right).$$

(ii) *Si* $u_n = \mathcal{O}(v_n)$ *et* $\sum v_n$ *diverge, alors*

$$\sum_{k=0}^{n} u_k = \mathcal{O}\left(\sum_{k=0}^{n} v_k\right).$$

(iii) *Si* $u_n \sim v_n$ *alors* $\sum u_n$ *et* $\sum v_n$ *sont de même nature.*

Les points (i) *et* (ii) *restent valables en remplaçant* $\mathcal{O}$ *par* o *ou* $\sim$.

Vocabulaire 25.10. $f : \mathbb{R}_+ \to \mathbb{R}$ $\mathcal{C}^0_{pm}$. *On dit que* $\int f$ *converge en* $+\infty$ *lorsque* $\lim_{x\to+\infty} \int_0^x f$ *existe et est réelle. On note alors*

$$\int_0^{+\infty} f = \lim_{x\to+\infty} \int_0^x f.$$

Proposition 25.11. $f : \mathbb{R}_+ \to \mathbb{R}$ $\mathcal{C}^0_{pm}$ *décroissante et positive.*

(i) *La série de terme général* $a_n = \int_n^{n+1} (f - f(n+1))$ *converge.*

(ii) $\sum f(n)$ *converge* ssi $\int f$ *converge en* $+\infty$.

(iii) *Si* $\sum f(n)$ *diverge alors* $\sum_{k=0}^{n} f(k) \sim \int_0^n f$.

Démonstration. (i) Montrer que $\forall n \in \mathbb{N}$, $f(n+1) \leqslant \int_n^{n+1} f \leqslant f(n)$; en déduire que $\forall n \in \mathbb{N}$, $0 \leqslant a_n \leqslant f(n) - f(n+1)$. Or, f est décroissante et positive donc admet une limite réelle en $+\infty$, donc la série de terme général $f(n) - f(n+1)$ converge, donc $\sum a_n$ aussi. (ii) Écrire $\sum_{k=0}^{n-1} a_k = \int_0^n f - \sum_{k=1}^{n} f(k)$. Or, la série de terme général a_n converge donc les suites $(\int_0^n f)$ et $(\sum_{k=1}^{n} f(k))$ sont de même nature. Montrer alors que $x \mapsto \int_0^x f$ a une limite réelle en $+\infty$ ssi $(\int_0^n f)$ converge, d'où le résultat. (iii) On a $\forall k \in \mathbb{N}$, $0 \leqslant a_k \leqslant f(k) - f(k+1)$. En supposant que $\sum f(n)$ diverge, écrire alors

$$0 \leqslant \underbrace{\int_0^n f - \sum_{k=1}^{n} f(k)}_{\sum_{k=0}^{n-1} a_k} \leqslant f(0) - f(n) \leqslant f(0) = o\left(\sum_{k=1}^{n} f(k)\right).$$

□

Proposition 25.12.

$$\sum_{k=1}^{n} \frac{1}{k} = \ln n + \gamma + \frac{1}{2n} + o\left(\frac{1}{n}\right),$$

où γ *est la* constante d'Euler.

Démonstration. Poser $u_n = \ln\left(1-\frac{1}{n}\right)+\frac{1}{n}$. Montrer d'abord que $\sum u_n$ converge et que $\sum_{k=n}^{\infty} u_k \sim -\frac{1}{2n}$. Écrire ensuite $\ln n = -\sum_{k=2}^{n} \ln\left(1-\frac{1}{k}\right)$, puis $\sum_{k=1}^{n} \frac{1}{k} - \ln n = 1 + \sum_{k=2}^{n} u_k$; en déduire le résultat souhaité. □

Proposition 25.13. *$\alpha \in \mathbb{R}$. Alors la série $\sum \frac{1}{n^\alpha}$, dite* série de Riemann*, converge* ssi *$\alpha > 1$.*

Démonstration. En notant $f_\alpha : x \in \mathbb{R}_+^* \longmapsto \frac{1}{x^\alpha}$, remarquer que $\sum f_\alpha(n)$ converge ssi $\int f_\alpha$ converge en $+\infty$. □

Proposition 25.14. *$(u_n) \in \mathbb{R}^{\mathbb{N}}$ et $\alpha \in \mathbb{R}$ t.q. $n^\alpha u_n \xrightarrow[n\to+\infty]{} \ell \in \mathbb{R}$.*

(i) *Si $\ell \neq 0$, alors $\sum u_n$ converge* ssi *$\alpha > 1$.*

(ii) *Si $\ell = 0$, $\alpha > 1$ et $u_n \geqslant 0$ à PCR, alors $\sum u_n$ converge.*

II.2 Critères de convergence

Proposition 25.15 (Critère de d'Alembert)**.** *$(u_n) \in \left(\mathbb{R}_+^*\right)^{\mathbb{N}}$ t.q. $\frac{u_{n+1}}{u_n} \xrightarrow[n\to+\infty]{} \ell \in \overline{\mathbb{R}}$. Alors :*

(i) *Si $\ell < 1$, alors $\sum u_n$ converge.*

(ii) *Si $\ell = 1$, alors $\sum u_n$ peut converger ou diverger.*

(iii) *Si $\ell > 1$, alors $\sum u_n$ diverge grossièrement.*

Proposition 25.16 (Critère de Cauchy)**.** *$(u_n) \in \left(\mathbb{R}_+^*\right)^{\mathbb{N}}$ t.q. $\sqrt[n]{u_n} \xrightarrow[n\to+\infty]{} \ell \in \overline{\mathbb{R}}$. Alors :*

(i) *Si $\ell < 1$, alors $\sum u_n$ converge.*

(ii) *Si $\ell = 1$, alors $\sum u_n$ peut converger ou diverger.*

(iii) *Si $\ell > 1$, alors $\sum u_n$ diverge grossièrement.*

II.3 Séries alternées

Vocabulaire 25.17 (Reste à l'ordre n)**.** *$(u_n) \in \mathbb{K}^{\mathbb{N}}$ t.q. $\sum_{k=0}^{\infty} u_k = S \in \mathbb{K}$, (S_n) la suite des sommes partielles associées à (u_n). Alors on appelle* reste à l'ordre *n de $\sum u_n$:*

$$R_n = S - S_n = \sum_{k=n+1}^{\infty} u_k.$$

Proposition 25.18. *$(a_n) \in (\mathbb{R}_+)^{\mathbb{N}}$ t.q. $(a_n) \searrow$ et $a_n \xrightarrow[n\to+\infty]{} 0$. Alors la série $\sum (-1)^n a_n$, dite* série alternée*, converge. De plus, pour tout $n \in \mathbb{N}$, $R_n = \sum_{k=n+1}^{\infty} (-1)^k a_k$ est du signe de $(-1)^{n+1}$ et $|R_n| \leqslant |a_{n+1}|$.*

Démonstration. En notant (S_n) la suite des sommes partielles associées à $((-1)^n a_n)$, montrer que les suites (S_{2n}) et (S_{2n+1}) sont adjacentes, et en déduire la convergence de $\sum (-1)^n a_n$. En notant $S = \lim_{n\to+\infty} S_n$, montrer alors que $0 \leqslant S - S_{2n+1} \leqslant a_{n+2}$ et que $0 \leqslant S_{2n} - S \leqslant a_{2n+1}$. □

III Séries à termes complexes

III.1 Généralités

Proposition 25.19. $(u_n) \in \mathbb{C}^{\mathbb{N}}$. $\sum u_n$ *converge* ssi $\sum \Re(u_n)$ *converge et* $\sum \Im(u_n)$ *converge.*

Définition 25.20 (Absolue convergence)**.** $(u_n) \in \mathbb{K}^{\mathbb{N}}$. *On dit que* $\sum u_n$ *est* absolument convergente *lorsque* $\sum |u_n|$ *converge.*

Proposition 25.21. $(u_n) \in \mathbb{K}^{\mathbb{N}}$. *Si* $\sum u_n$ *est absolument convergente alors* $\sum u_n$ *converge.*

Démonstration. *Première étape* : $\mathbb{K} = \mathbb{R}$. Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$ t.q. $\sum u_n$ est absolument convergente. Poser $u_n^+ = \max(u_n, 0)$ et $u_n^- = \max(-u_n, 0)$. On a alors $u_n = u_n^+ - u_n^-$ et $|u_n| = u_n^+ + u_n^-$. Écrire alors $0 \leqslant u_n^+ \leqslant |u_n|$ et $0 \leqslant u_n^- \leqslant |u_n|$. Or $\sum |u_n|$ converge donc $\sum u_n^+$ et $\sum u_n^-$ convergent, d'où $\sum u_n = \sum (u_n^+ - u_n^-)$ converge. *Deuxième étape* : $\mathbb{K} = \mathbb{C}$. Soit $(u_n) \in \mathbb{C}^{\mathbb{N}}$ t.q. $\sum u_n$ est absolument convergente. Comme $0 \leqslant |\Re(u_n)| \leqslant |u_n|$ et $0 \leqslant |\Im(u_n)| \leqslant |u_n|$, $\sum |\Re(u_n)|$ et $\sum |\Im(u_n)|$ convergent. D'après la première étape, $\sum \Re(u_n)$ et $\sum \Im(u_n)$ convergent, donc $\sum u_n$ converge. □

III.2 Quelques propriétés

Proposition 25.22. *L'ensemble* $\left\{(u_n) \in \mathbb{K}^{\mathbb{N}},\ \sum u_n \text{ est absolument convergente}\right\}$ *est un* $\mathbb{K}$*-espace vectoriel.*

Proposition 25.23. $(u_n) \in \mathbb{K}^{\mathbb{N}}$, $(v_n) \in \mathbb{R}^{\mathbb{N}}$ *t.q.* $v_n \geqslant 0$ *à PCR.*

(i) *Si* $u_n = \mathcal{O}(v_n)$ *et* $\sum v_n$ *converge alors* $\sum u_n$ *est absolument convergente. Dans ce cas*

$$\sum_{k=n}^{\infty} u_k = \mathcal{O}\left(\sum_{k=n}^{\infty} v_k\right).$$

(ii) *Si* $u_n = \mathcal{O}(v_n)$ *et* $\sum v_n$ *diverge, alors*

$$\sum_{k=0}^{n} u_k = \mathcal{O}\left(\sum_{k=0}^{n} v_k\right).$$

Ceci reste valable en remplaçant $\mathcal{O}$ *par* o *ou* $\sim$.

III.3 Exemples classiques

Théorème 25.24 (Théorème de Cesàro)**.** $(u_n) \in \mathbb{K}^{\mathbb{N}}$.

$$u_n \xrightarrow[n\to+\infty]{} \ell \in \mathbb{K} \Longrightarrow \frac{1}{n+1}\sum_{k=0}^{n} u_k \xrightarrow[n\to+\infty]{} \ell.$$

Démonstration. Comme $u_n - \ell = o(1)$ et que $\sum 1$ diverge, $\sum_{k=0}^{n}(u_k - \ell) = o\left(\sum_{k=0}^{n} 1\right) = o(n)$, donc $\frac{1}{n+1}\sum_{k=0}^{n} u_k = \ell + o(1)$. □

Théorème 25.25 (Formule de Stirling)**.**

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Démonstration. On note $u_n = \frac{n!}{\sqrt{n}}\left(\frac{e}{n}\right)^n$, $v_n = \ln u_n - \ln u_{n-1}$. Montrer que $v_n = \mathcal{O}\left(\frac{1}{n^2}\right)$. Comme $\sum \frac{1}{n^2}$ converge, en déduire que $\sum v_n$ converge, donc $(\ln u_n)$ converge, d'où $u_n \xrightarrow[n\to+\infty]{} C \in \mathbb{R}_+^*$. Reste à déterminer C. On pose pour cela $I_n = \int_0^{\frac{\pi}{2}} \sin^n t \, \mathrm{d}t$. Montrer premièrement que $\forall n \in \mathbb{N}$, $I_{n+2} = \frac{n+1}{n+2} I_n$. En déduire que $\forall n \in \mathbb{N}$, $I_{2n} = \frac{(2n)!}{(2^n n!)^2} \cdot \frac{\pi}{2}$. Montrer ensuite que $(I_n) \searrow$ et que $I_n \sim I_{n+1}$. De plus, en notant $\alpha_n = (n+1) I_n I_{n+1}$, montrer que $\forall n \in \mathbb{N}$, $\alpha_{n+1} = \alpha_n$ donc $\forall n \in \mathbb{N}$, $\alpha_n = \alpha_0 = \frac{\pi}{2}$. Or $\alpha_n \sim n I_n^2$, d'où $I_n \sim \sqrt{\frac{\pi}{2n}}$. En déduire que $C = \sqrt{2\pi}$. □

IV Séries de vecteurs et de matrices

Notation 25.26. *Par la suite, on notera* $\mathbb{E} = \mathbb{K}^p$ ou $\mathbb{M}_{n,p}(\mathbb{K})$.

Définition 25.27 (Convergence vectorielle et matricielle)**.** $(u_n) \in \mathbb{E}^{\mathbb{N}}$. *On dit que* (u_n) converge *(resp. diverge) lorsque les suites des composantes de* (u_n) *dans la base canonique convergent (resp. divergent) dans* $\mathbb{K}$. *On dit de même que* $\sum u_n$ converge *(resp. diverge) lorsque les suites des composantes de* $\left(\sum_{k=0}^n u_k\right)$ *dans la base canonique convergent (resp. divergent) dans* $\mathbb{K}$.

Définition 25.28 (Normes infinies)**.** *On définit les normes* $\|\cdot\|_\infty$ *et* $|||\cdot|||_\infty$ *par :*

(i) *Pour* $x = (x_1, \ldots, x_p) \in \mathbb{K}^p$ *:*

$$\|x\|_\infty = \max_{1 \leqslant i \leqslant p} |x_i| .$$

(ii) *Pour* $A \in \mathbb{M}_{n,p}(\mathbb{K})$ *:*

$$|||A|||_\infty = \sup_{X \neq 0} \frac{\|AX\|_\infty}{\|X\|_\infty}.$$

On notera $\|\cdot\| = \|\cdot\|_\infty$ ou $|||\cdot|||_\infty$.

Lemme 25.29. $A = (a_{ij}) \in \mathbb{M}_{n,p}(\mathbb{K})$. $|||A|||_\infty = \max_{1 \leqslant i \leqslant n} \sum_{1 \leqslant j \leqslant p} |a_{ij}|$.

Proposition 25.30. $(u_n) \in \mathbb{E}^{\mathbb{N}}$. *Alors* $u_n \xrightarrow[n\to+\infty]{} u \in \mathbb{E}$ ssi $\|u_n - u\| \xrightarrow[n\to+\infty]{} 0$.

Proposition 25.31. $\left\{(u_n) \in \mathbb{E}^{\mathbb{N}},\ (u_n) \text{ converge}\right\}$ *et* $\left\{(u_n) \in \mathbb{E}^{\mathbb{N}},\ \sum u_n \text{ converge}\right\}$ *sont des* $\mathbb{K}$*-espaces vectoriels.*

Définition 25.32 (Absolue convergence)**.** $(u_n) \in \mathbb{E}^{\mathbb{N}}$. *On dit que* $\sum u_n$ *est* absolument convergente *lorsque* $\sum \|u_n\|$ *converge.*

Proposition 25.33. $(u_n) \in \mathbb{E}^{\mathbb{N}}$. *Si* $\sum u_n$ *est absolument convergente alors* $\sum u_n$ *converge.*

Lemme 25.34. $\forall (U, V) \in \mathbb{M}_p(\mathbb{K})^2$, $|||UV|||_\infty \leqslant |||U|||_\infty \cdot |||V|||_\infty$.

Proposition 25.35. $A \in \mathbb{M}_p(\mathbb{K})$. *Si* $|||A|||_\infty < 1$, *alors* $(I_p - A) \in GL_p(\mathbb{K})$, $\sum A^n$ *converge et :*

$$(I_p - A)^{-1} = \sum_{k=0}^{\infty} A^k.$$

Démonstration. Comme $\left|\left|\left|A^k\right|\right|\right|_\infty \leqslant |||A|||_\infty^k$, $\sum A^n$ est absolument convergente donc convergente. En notant $S_n = \sum_{k=0}^n A^k$ et $S = \lim_{n\to+\infty} S_n$, on a $(I_p - A)S_n = I_p - A^{n+1} \xrightarrow[n\to+\infty]{} I_p$. Montrer alors que $(I_p - A)S_n \xrightarrow[n\to+\infty]{} (I_p - A)S$ en utilisant le lemme 25.34, puis en déduire le résultat. □

Proposition 25.36. *$A \in \mathbb{M}_p(\mathbb{K})$. Alors $\sum \frac{A^n}{n!}$ converge et on note :*

$$\exp A = \sum_{k=0}^{\infty} \frac{A^k}{k!}.$$

Démonstration. Utiliser le fait que $\left|\left|\left| \frac{A^k}{k!} \right|\right|\right|_\infty \leqslant \frac{|||A|||_\infty^k}{k!}$. □

Chapitre 26

Intégration sur un Intervalle Quelconque

I Retour sur les fonctions en escaliers ou continues par morceaux

Définition 26.1 (Fonction en escaliers ou continue par morceaux)**.** *$f : I \to \mathbb{R}$ est dite* en escaliers *(resp. $\mathcal{C}^0_{pm}$) sur I lorsque f est en escaliers (resp. $\mathcal{C}^0_{pm}$) sur tout segment inclus dans I. De plus, $f : I \to \mathbb{C}$ est dite $\mathcal{C}^0_{pm}$ lorsque $\Re(f)$ et $\Im(f)$ le sont.*

Proposition 26.2. *L'ensemble $\left\{f \in \mathbb{K}^I,\ f\ \mathcal{C}^0_{pm}\ \text{sur}\ I\right\}$ est un $\mathbb{K}$-espace vectoriel.*

II Intégrale généralisée sur $[a, +\infty[$

II.1 Généralités

Définition 26.3 (Convergence de $\int f$)**.** *$f : [a, +\infty[\to \mathbb{K}\ \mathcal{C}^0_{pm}$. On dit que $\int f$ converge en $+\infty$ lorsque $\lim_{x\to+\infty} \int_a^x f$ existe et est finie. On note alors*

$$\int_a^{+\infty} f = \lim_{x\to+\infty} \int_a^x f.$$

Proposition 26.4. *$f : [a, +\infty[\to \mathbb{K}\ \mathcal{C}^0_{pm}$. Alors $\int f$ converge en $+\infty$* ssi *il existe $c \in [a, +\infty[$ t.q. la fonction $x \longmapsto \int_c^x f$ a une limite finie en $+\infty$. Dans ce cas, $\forall c \in [a, +\infty[, x \longmapsto \int_c^x f$ a une lim*

Proposition 26.5. *$\mathcal{I} = \left\{f \in \mathcal{C}^0_{pm}\left([a, +\infty[, \mathbb{K}\right),\ \int f \text{ converge en } +\infty\right\}$ est un $\mathbb{K}$-espace vectoriel et l'application $f \in \mathcal{I} \longmapsto \int_a^{+\infty} f$ est une forme linéaire.*

Proposition 26.6. *$f : [a, +\infty[\to \mathbb{R}\ \mathcal{C}^0_{pm}$. On suppose que $\int f$ converge en $+\infty$ et $f \geqslant 0$ sur $[a, +\infty[$.*

(i) *$\int_a^{+\infty} f \geqslant 0$.*

(ii) *Si de plus f est $\mathcal{C}^0$ sur $[a, +\infty[$, alors $\int_a^{+\infty} f = 0 \Longrightarrow f = 0$ sur $[a, +\infty[$.*

Proposition 26.7. *$f : [a, +\infty[\to \mathbb{K}\ \mathcal{C}^0$ t.q. $\int f$ converge en $+\infty$. Alors la fonction*

$$F : x \in [a, +\infty[\longmapsto \int_x^{+\infty} f$$

est $\mathcal{C}^1$ sur $[a, +\infty[$ et vérifie $F' = -f$.

Proposition 26.8. *$f : [a, +\infty[\to \mathbb{K}\ \mathcal{C}^0_{pm}$ positive. Alors $\int f$ converge en $+\infty$* ssi *$x \in [a, +\infty[\longmapsto \int_a^x f$ est majorée.*

II.2 Relations de comparaison et fonctions de référence

Proposition 26.9. *$\alpha \in \mathbb{R}$. Soit $f_\alpha : t \in [1, +\infty[\longmapsto \frac{1}{t^\alpha}$. Alors $\int f_\alpha$ converge en $+\infty$* ssi *$\alpha > 1$.*

Proposition 26.10. *$f, g : [a, +\infty[\to \mathbb{K}$ $\mathcal{C}^0_{pm}$ positives.*

(i) *Si $0 \leqslant f \leqslant g$ et $\int g$ converge en $+\infty$ alors $\int f$ converge en $+\infty$.*

(ii) *Si $f = \mathcal{O}_{+\infty}(g)$ et $\int g$ converge en $+\infty$ alors $\int f$ converge en $+\infty$.*

(iii) *Si $f \underset{+\infty}{\sim} g$, alors $\int f$ et $\int g$ sont de même nature en $+\infty$.*

III Intégrabilité d'une fonction sur $[a, +\infty[$

Définition 26.11 (Intégrabilité)**.** *$f : [a, +\infty[\to \mathbb{K}$ $\mathcal{C}^0_{pm}$. On dit que f est* intégrable *sur $[a, +\infty[$ lorsque $\int |f|$ converge en $+\infty$.*

Proposition 26.12. *$f : [a, +\infty[\to \mathbb{K}$ $\mathcal{C}^0_{pm}$. Si f est intégrable sur $[a, +\infty[$, alors $\int f$ converge en $+\infty$.*

Démonstration. Comme pour la proposition 25.21. □

IV Intégration sur un intervalle semi-ouvert

IV.1 Généralités

Définition 26.13 (Convergence de $\int f$)**.**

(i) *$f : [a, b[\to \mathbb{K}$ $\mathcal{C}^0_{pm}$. On dit que $\int_a^b f$ converge lorsque $\lim_{x \to b} \int_a^x f$ existe et est finie. On note alors*
$$\int_a^b f = \lim_{x \to b} \int_a^x f.$$

(ii) *$f :]a, b] \to \mathbb{K}$ $\mathcal{C}^0_{pm}$. On dit que $\int_a^b f$ converge lorsque $\lim_{x \to a} \int_x^b f$ existe et est finie. On note alors*
$$\int_a^b f = \lim_{x \to a} \int_x^b f.$$

Proposition 26.14.

(i) *$f : [a, b[\to \mathbb{K}$ $\mathcal{C}^0_{pm}$ positive. Alors $\int_a^b f$ converge* ssi *la fonction $x \in [a, b[\longmapsto \int_a^x f$ est majorée.*

(ii) *$f :]a, b] \to \mathbb{K}$ $\mathcal{C}^0_{pm}$ positive. Alors $\int_a^b f$ converge* ssi *la fonction $x \in]a, b] \longmapsto \int_x^b f$ est majorée.*

IV.2 Intégrabilité

Définition 26.15 (Intégrabilité)**.** *$f : [a, b[\to \mathbb{K}$ (resp. $f :]a, b] \to \mathbb{K}$) $\mathcal{C}^0_{pm}$. On dit que f est* intégrable *sur $[a, b[$ (resp. $]a, b]$) lorsque $\int_a^b |f|$ converge.*

Proposition 26.16. *$f : [a, b[\to \mathbb{K}$ (resp. $f :]a, b] \to \mathbb{K}$) $\mathcal{C}^0_{pm}$. Si f est intégrable sur $[a, b[$ (resp. $]a, b]$), alors $\int_a^b f$ converge.*

IV.3 Relations de comparaison et fonctions de référence

Proposition 26.17. *$f, g : [a, b[\to \mathbb{K}$ (resp. $f, g :]a, b] \to \mathbb{K}$) $\mathcal{C}^0_{pm}$. Si $0 \leqslant f \leqslant g$ sur $[a, b[$ (resp. $]a, b]$) et $\int_a^b g$ converge alors $\int_a^b f$ converge. Ceci reste valable en remplaçant $\leqslant$ par $\mathcal{O}$, o ou $\sim$.*

Proposition 26.18. *$\alpha \in \mathbb{R}$. Soit $f_\alpha : t \in]a, b] \longmapsto \frac{1}{(t-a)^\alpha}$. Alors $\int_a^b f_\alpha$ converge* ssi *$\alpha < 1$.*

V Intégration sur un intervalle quelconque

Définition 26.19 (Convergence de $\int f$)**.**

(i) *$f :]a, b[\to \mathbb{K}$ $\mathcal{C}^0_{pm}$. On dit que $\int_a^b f$ converge lorsqu'il existe $c \in]a, b[$ t.q. $\int_a^c f$ et $\int_c^b f$ convergent. Dans ce cas, on note*

$$\int_a^b f = \int_a^c f + \int_c^b f.$$

(ii) *$f :]a, b[\cup]b, c[\to \mathbb{K}$ $\mathcal{C}^0_{pm}$. On dit que $\int_a^c f$ converge lorsque $\int_a^b f$ et $\int_b^c f$ convergent. On dit de plus que f est intégrable sur $]a, c[$ lorsque $\int_a^c |f|$ converge.*

Proposition 26.20. *$\left\{ f \in \mathcal{C}^0_{pm}(]a, b[, \mathbb{K}),\ \int_a^b f \text{ converge} \right\}$ est un $\mathbb{K}$-espace vectoriel.*

Proposition 26.21. *$f :]a, b[\to \mathbb{R}$ $\mathcal{C}^0_{pm}$. On suppose que $\int_a^b f$ converge et $f \geqslant 0$ sur $]a, b[$.*

(i) *$\int_a^b f \geqslant 0$.*

(ii) *Si de plus f est $\mathcal{C}^0$ sur $]a, b[$, alors $\int_a^b f = 0 \Longrightarrow f = 0$ sur $]a, b[$.*

Proposition 26.22. *$f :]a, b[\to \mathbb{R}$ $\mathcal{C}^0_{pm}$. $(a_n) \in]a, b[^{\mathbb{N}}\searrow$, $(b_n) \in]a, b[^{\mathbb{N}}\nearrow$ avec $a_n \xrightarrow[n\to+\infty]{} a$ et $b_n \xrightarrow[n\to+\infty]{} b$.*

(i) *Si $\int_a^b f$ converge, alors la suite $\left(\int_{a_n}^{b_n} f\right)$ converge.*

(ii) *Si $f \geqslant 0$, alors $\int_a^b f$ converge* ssi *la suite $\left(\int_{a_n}^{b_n} f\right)$ converge.*

VI Intégration par parties et intégration par substitution

Proposition 26.23 (Intégration par parties)**.** *$u, v :]a, b[\to \mathbb{K}$ $\mathcal{C}^1$. Si (uv) admet des limites finies en a et b, alors $\int_a^b u'v$ et $\int_a^b uv'$ sont de même nature. Dans ce cas, et si les deux intégrales convergent, on a :*

$$\int_a^b u'v = [uv]_a^b - \int_a^b uv'.$$

Proposition 26.24 (Intégration par substitution)**.** *$f : I \to \mathbb{R}$ $\mathcal{C}^0$, $\varphi : J \to I$ $\mathcal{C}^1$ et bijective. Alors $\int_I f$ et $\int_J (f \circ \varphi)\varphi'$ sont de même nature, et en cas de convergence :*

$$\int_I f = \int_J (f \circ \varphi)\,|\varphi'|\,.$$

Ainsi, en notant $J = (\alpha, \beta)$, on a :

$$\int_{\lim_\alpha \varphi}^{\lim_\beta \varphi} f = \int_\alpha^\beta (f \circ \varphi)\varphi'.$$

VII Quelques compléments

VII.1 Fonctions à carré intégrable

Vocabulaire 26.25 (Fonction à carré intégrable)**.** $f : I \to \mathbb{C}$ $\mathcal{C}^0$. *f est dite* à carré intégrable *lorsque f^2 est intégrable sur I (i.e. $\int_I |f|^2$ converge). On note $\mathcal{L}^2_I$ l'ensemble des fonctions à carré intégrable sur I.*

Proposition 26.26. *$(f, g) \in \left(\mathcal{L}^2_I\right)^2$. Alors (fg) est intégrable sur I et :*

$$\int_I |fg| \leqslant \sqrt{\int_I |f|^2}\sqrt{\int_I |g|^2}.$$

Démonstration. Démontrer l'intégrabilité de (fg) en utilisant le fait que $0 \leqslant |fg| \leqslant \frac{1}{2}\left(|f|^2 + |g|^2\right)$, puis utiliser l'inégalité de Cauchy-Schwarz sur un segment (proposition 24.38). □

VII.2 Fonction gamma

Définition 26.27 (Fonction gamma)**.** *On définit :*

$$\Gamma : \alpha \in \mathbb{R}_+^* \longmapsto \int_0^{+\infty} x^{\alpha-1}e^{-x}\,\mathrm{d}x.$$

Proposition 26.28.

(i) $\forall \alpha \in \mathbb{R}_+^*$, $\Gamma(\alpha + 1) = \alpha\Gamma(\alpha)$.

(ii) $\forall n \in \mathbb{N}^*$, $\Gamma(n) = (n-1)!$.

(iii) $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$.

(iv) Γ *est convexe sur* $\mathbb{R}_+^*$.

(v) $\lim_{+\infty} \Gamma = +\infty$.

(vi) $\lim_{0^+} \Gamma = +\infty$.

Démonstration. (i) Intégrer par parties. (iii) Admettre $\int_0^\infty e^{-u^2}\,\mathrm{d}u = \frac{\sqrt{\pi}}{2}$. (iv) Montrer que la fonction $\psi : \alpha \in \mathbb{R}_+^* \longmapsto x^{\alpha-1}$ est convexe (en calculant ψ''). Soit $(\alpha, \beta) \in \left(\mathbb{R}_+^*\right)^2$; écrire $\forall \lambda \in [0,1]$, $\lambda\psi(\alpha) + (1-\lambda)\psi(\beta) \geqslant \psi(\lambda\alpha + (1-\lambda)\beta)$. En déduire alors que $\forall \lambda \in [0,1]$, $\lambda\Gamma(\alpha) + (1-\lambda)\Gamma(\beta) \geqslant \Gamma(\lambda\alpha + (1-\lambda)\beta)$. (v) Utiliser la convexité de Γ pour écrire $\frac{\Gamma(\alpha)-\Gamma(2)}{\alpha-2} \geqslant \frac{\Gamma(3)-\Gamma(2)}{3-2}$, et en déduire une minoration de Γ. (vi) Montrer que $\Gamma(\alpha) \geqslant \frac{1}{e}\int_0^1 x^{\alpha-1} \xrightarrow[\alpha\to 0^+]{} +\infty$. □

VIII Formules de quadrature

VIII.1 Le théorème de Weierstrass

Théorème 26.29 (Théorème de Weierstrass)**.** *$f : [a, b] \to \mathbb{R}$ $\mathcal{C}^0$. Alors il existe une suite (P_n) de polynômes convergeant uniformément vers f sur $[a, b]$:*

$$\sup_{[a,b]} |f - P_n| \xrightarrow[n\to+\infty]{} 0.$$

Démonstration. *Première étape.* Pour $n \in \mathbb{N}$, on pose

$$f_n : x \in \mathbb{R} \longmapsto \begin{cases} (1-x^2)^n \text{ si } |x| < 1 \\ 0 \text{ sinon} \end{cases} \quad \text{et} \quad \mu_n = \int_{-1}^{1} f_n \quad \text{et} \quad \varphi_n = \frac{f_n}{\mu_n}.$$

Noter que $\int_{-1}^{1} \varphi_n = 1$. Montrer que $\int_0^1 f_n \xrightarrow[n\to+\infty]{} 0$ et en déduire que $\mu_n \xrightarrow[n\to+\infty]{} 0$. Montrer ensuite que $\mu_n \geqslant 2\int_0^1 (1-x)^n \, \mathrm{d}x = \frac{2}{n+1}$ et en déduire :

$$\forall x \in [-1,1],\ \varphi_n(x) \xrightarrow[n\to+\infty]{} \begin{cases} 0 \text{ si } x \neq 0 \\ +\infty \text{ si } x = 0 \end{cases}.$$

Deuxième étape. Soit $f : [0,1] \to \mathbb{R}$ $\mathcal{C}^0$. Poser

$$P_n : \xi \in [0,1] \longmapsto \int_0^1 f(x)\varphi_n(\xi - x) \, \mathrm{d}x.$$

Montrer premièrement que P_n est polynomiale. Soit $\xi \in [a,b] \subset]0,1[$ et $\delta > 0$. Montrer que $\sup_{[\delta,1]} |\varphi_n| = \varphi_n(\delta) \xrightarrow[n\to+\infty]{} 0$, et de même sur $[-1,-\delta]$, d'où (φ_n) converge uniformément vers 0 sur $[-1,-\delta]\cup[\delta,1]$. En notant $I_1 =]\xi-\delta, \xi+\delta[$ (qui est inclus dans $[0,1]$ en choisissant $\delta < \min(a, 1-b)$), et $I_2 = [0, \xi-\delta] \cup [\xi+\delta, 1]$, on a donc $\int_{I_2} f(x)\varphi_n(\xi-x) \, \mathrm{d}x \xrightarrow[n\to+\infty]{} 0$ (indépendamment de ξ). Écrire alors

$$\begin{aligned} P_n(\xi) - f(\xi) = {} & \overbrace{\int_{I_2} f(x)\varphi_n(\xi-x) \, \mathrm{d}x}^{A_n} \\ & + \underbrace{\int_{I_1} f(x)\varphi_n(\xi-x) \, \mathrm{d}x - \int_{I_1} f(\xi)\varphi_n(\xi-x) \, \mathrm{d}x}_{B_n} + \underbrace{\int_{I_1} f(\xi)\varphi_n(\xi-x) \, \mathrm{d}x - f(\xi)}_{C_n}. \end{aligned}$$

Soit $\varepsilon > 0$. En utilisant l'uniforme continuité de f sur $[0,1]$ (par le théorème de Heine), obtenir l'existence d'un $\eta > 0$ t.q. $\forall (x,y) \in [0,1]^2$, $|x-y| \leqslant \eta \Longrightarrow |f(x) - f(y)| \leqslant \varepsilon$ et montrer que $|B_n| \leqslant \varepsilon$ (en choisissant $\delta < \eta$). Montrer de plus que $\exists n_0 \in \mathbb{N}$, $\forall n \geqslant n_0$, $|A_n| \leqslant \varepsilon$ et $\exists n_1 \in \mathbb{N}$, $\forall n \geqslant n_1$, $|C_n| \leqslant \varepsilon$, où n_0 et n_1 ne dépendent pas de ξ, et en déduire que $\exists n_2 \in \mathbb{N}$, $\forall n \geqslant n_2$, $\forall \xi \in [a,b]$, $|f(\xi) - P_n(\xi)| \leqslant \varepsilon$. Cela montre que $\sup_{[a,b]} |f - P_n| \xrightarrow[n\to+\infty]{} 0$. Ainsi, (P_n) converge uniformément vers f sur tout segment $[a,b] \subset]0,1[$. Quitte à prolonger f sur un intervalle contenant $[0,1]$ et à appliquer ce qui précède, on obtient ainsi que (P_n) converge uniformément vers f sur $[0,1]$, ce qu'on peut généraliser à tout segment par translation. □

Remarque 26.30. *Sur $\mathbb{R}$, f ne peut pas être limite uniforme d'une suite de polynômes, sauf si f est polynomiale.*

VIII.2 Formules de quadrature

Proposition 26.31. *$f : [a,b] \to \mathbb{R}$ $\mathcal{C}^0$. Pour $n \in \mathbb{N}^*$, soit $\left(x_1^{(n)}, \ldots, x_n^{(n)}\right) \in [a,b]^n$, $\left(\omega_1^{(n)}, \ldots, \omega_n^{(n)}\right) \in \mathbb{R}^n$, et $Q_n : g \in \mathbb{R}^{[a,b]} \longmapsto \sum_{i=1}^n \omega_i^{(n)} g\left(x_i^{(n)}\right)$. On suppose que :*

(i) $\exists M \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $\sum_{i=1}^n \left|\omega_i^{(n)}\right| \leqslant M$.

(ii) $\forall P \in \mathbb{R}[X]$, $Q_n(P) \xrightarrow[n\to+\infty]{} \int_a^b P$.

Alors

$$Q_n(f) \xrightarrow[n\to+\infty]{} \int_a^b f.$$

Théorème 26.32. *$f : [a, b] \to \mathbb{R}$. Pour $n \in \mathbb{N}^*$, $i \in [\![0, n]\!]$, on pose $a_i = a + i\frac{b-a}{n}$.*

(i) Méthode des rectangles. *Si f est $\mathcal{C}^1$, alors*

$$\left| \int_a^b f - \frac{b-a}{n} \sum_{i=0}^{n-1} f(a_i) \right| = \mathcal{O}\left(\frac{1}{n}\right).$$

(ii) Méthode des trapèzes. *Si f est $\mathcal{C}^2$, alors*

$$\left| \int_a^b f - \frac{b-a}{n} \left(\frac{1}{2} f(a) + \sum_{i=1}^{n-1} f(a_i) + \frac{1}{2} f(b) \right) \right| = \mathcal{O}\left(\frac{1}{n^2}\right).$$

Chapitre 27

Espaces Préhilbertiens

I Généralités

I.1 Quelques définitions

Définition 27.1 (Forme bilinéaire)**.** *E et F deux $\mathbb{R}$-espaces vectoriels. $\varphi : E \times F \to \mathbb{R}$ est dite* bilinéaire *lorsque pour tout $x \in E$, $\begin{vmatrix} F \longrightarrow \mathbb{R} \\ y \longmapsto \varphi(x,y) \end{vmatrix}$ est linéaire et pour tout $y \in F$, $\begin{vmatrix} E \longrightarrow \mathbb{R} \\ x \longmapsto \varphi(x,y) \end{vmatrix}$ est linéaire.*

Définition 27.2 (Formes bilinéaires particulières)**.** *E un $\mathbb{R}$-espace vectoriel et $\varphi : E \times E \to \mathbb{R}$ une forme bilinéaire.*

(i) *φ est dite* symétrique *lorsque* $\forall (x,y) \in E^2,\ \varphi(x,y) = \varphi(y,x)$.

(ii) *φ est dite* positive *lorsque* $\forall x \in E,\ \varphi(x,x) \geqslant 0$.

(iii) *φ est dite* définie *lorsque* $\forall x \in E,\ \varphi(x,x) = 0 \Longrightarrow x = 0$.

Définition 27.3 (Produit scalaire)**.** *E un $\mathbb{R}$-espace vectoriel et $\varphi : E \times E \to \mathbb{R}$ une forme bilinéaire. On dit que φ est un* produit scalaire *lorsque φ est symétrique, positive et définie.*

Exemple 27.4. *Quelques produits scalaires classiques :*

(i) $(x,y) \in (\mathbb{R}^n)^2 \longmapsto \sum_{i=1}^n x_i y_i$, *avec* $x = (x_1, \ldots, x_n)$ *et* $y = (y_1, \ldots, y_n)$.

(ii) $(A,B) \in \mathbb{M}_n(\mathbb{R})^2 \longmapsto \operatorname{tr}({}^tAB)$.

(iii) $(P,Q) \in \mathbb{R}_n[X]^2 \longmapsto \sum_{k=0}^n P(k)Q(k)$.

(iv) $(P,Q) \in \mathbb{R}[X]^2 \longmapsto \int_{-1}^1 \frac{P(t)Q(t)}{\sqrt{1-t^2}}\,\mathrm{d}t$.

(v) $(f,g) \in \mathcal{C}^\infty([0,1],\mathbb{R}) \longmapsto \int_0^1 fg$.

(vi) $(f,g) \in \mathcal{L}^2_I \longmapsto \int_I fg$.

Définition 27.5 (Norme)**.** *E un $\mathbb{R}$-espace vectoriel. On dit que $\mathfrak{N} : E \to \mathbb{R}$ est une* norme *lorsque les quatre propriétés suivantes sont vérifiées :*

(i) $\forall x \in E,\ \mathfrak{N}(x) \geqslant 0$,

(ii) $\forall x \in E,\ \mathfrak{N}(x) = 0 \Longleftrightarrow x = 0$,

(iii) $\forall x \in E,\ \forall \lambda \in \mathbb{R},\ \mathfrak{N}(\lambda x) = |\lambda| \cdot \mathfrak{N}(x)$,

(iv) $\forall (x,y) \in E^2,\ \mathfrak{N}(x+y) \leqslant \mathfrak{N}(x) + \mathfrak{N}(y)$.

I.2 Cauchy-Schwarz et conséquences

Proposition 27.6. *E un $\mathbb{R}$-espace vectoriel et $\langle\cdot,\cdot\rangle$ un produit scalaire sur E. On pose, pour $x \in E$, $\|x\| = \sqrt{\langle x, x\rangle}$. Alors :*

(i) $\|x+y\|^2 = \|x\|^2 + 2\langle x, y\rangle + \|y\|^2$,

(ii) $\|x-y\|^2 = \|x\|^2 - 2\langle x, y\rangle + \|y\|^2$,

(iii) $\langle x, y\rangle = \frac{1}{2}\left(\|x+y\|^2 - \|x\|^2 - \|y\|^2\right)$,

(iv) $\langle x, y\rangle = \frac{1}{4}\left(\|x+y\|^2 - \|x-y\|^2\right)$.

L'égalité (iv) *est appelée* identité de polarisation.

Proposition 27.7 (Inégalité de Cauchy-Schwarz)**.** *E un $\mathbb{R}$-espace vectoriel et $\langle\cdot,\cdot\rangle$ un produit scalaire sur E. On pose, pour $x \in E$, $\|x\| = \sqrt{\langle x, x\rangle}$. Alors :*

$$\forall (x, y) \in E^2,\ |\langle x, y\rangle| \leqslant \|x\| \cdot \|y\|,$$

avec égalité ssi *x et y sont colinéaires.*

Démonstration. Supposer $x \neq 0$ et $y \neq 0$ (sinon le résultat reste vrai). Poser alors $x' = \frac{x}{\|x\|}$, $y' = \frac{y}{\|y\|}$. Utiliser le fait que $\langle x', y'\rangle = \frac{1}{2}\left(\|x'+y'\|^2 - 2\right)$ pour montrer que $|\langle x', y'\rangle| \leqslant 1$ et en déduire le résultat. □

Proposition 27.8 (Inégalité de Minkowski)**.** *E un $\mathbb{R}$-espace vectoriel et $\langle\cdot,\cdot\rangle$ un produit scalaire sur E. On pose, pour $x \in E$, $\|x\| = \sqrt{\langle x, x\rangle}$. Alors $\|\cdot\|$ est une norme. En particulier :*

$$\forall (x, y) \in E^2,\ \|x+y\| \leqslant \|x\| + \|y\|,$$

avec égalité ssi *x et y sont positivement colinéaires (i.e. $x = 0$ ou $\exists \lambda \in \mathbb{R}_+,\ y = \lambda x$).*

Définition 27.9 (Norme hilbertienne)**.** *E un $\mathbb{R}$-espace vectoriel. On dit qu'une norme $\mathfrak{N} : E \to \mathbb{R}$ est* hilbertienne *s'il existe un produit scalaire $\varphi : E \times E \to \mathbb{R}$ t.q. $\forall x \in E$, $\mathfrak{N}(x) = \sqrt{\varphi(x, x)}$.*

Proposition 27.10 (Identité du parallélogramme)**.** *E un $\mathbb{R}$-espace vectoriel, $\|\cdot\|$ une norme hilbertienne.*

$$\forall (x, y) \in E^2,\ \|x+y\|^2 + \|x-y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right).$$

II Orthogonalité

II.1 Généralités

Définition 27.11 (Espaces préhilbertiens et euclidiens)**.** *Un* espace préhilbertien *est un espace vectoriel réel muni d'un produit scalaire. Un espace préhilbertien de dimension finie est dit* euclidien.

Définition 27.12 (Vecteurs orthogonaux, etc.)**.** *E un espace préhilbertien muni d'un produit scalaire $\langle\cdot,\cdot\rangle$.*

(i) *Deux vecteurs $x \in E$, $y \in E$ sont dits* orthogonaux *lorsque $\langle x, y\rangle = 0$. On note alors $x \perp y$.*

(ii) *Une famille $(x_i)_{i\in I}$ est dite* orthogonale *lorsque $\forall (i, j) \in I^2$, $i \neq j \Longrightarrow x_i \perp x_j$.*

(iii) *Une famille* $(x_i)_{i\in I}$ *est dite* orthonormale *lorsque* $\forall (i,j)\in I^2,\ \langle x_i, x_j\rangle = \delta_{ij}$.

(iv) *Pour* $A\subset E$, *on note* $A^\perp = \{x\in E,\ \forall a\in A,\ x\perp a\}$.

(v) *Deux sous-espaces vectoriels* F *et* G *de* E *sont dits* orthogonaux *lorsque tout vecteur de* F *est orthogonal à tout vecteur de* G.

Proposition 27.13. *E un espace préhilbertien.*

(i) *Toute famille orthogonale de vecteurs non nuls de E est libre.*

(ii) *Toute famille orthonormale de vecteurs de E est libre.*

Théorème 27.14 (Théorème de Pythagore)**.** *E un espace préhilbertien. $(x_1,\dots,x_n)$ une famille orthogonale de E. Alors*

$$\left\|\sum_{i=1}^n x_i\right\|^2 = \sum_{i=1}^n \|x_i\|^2 .$$

Démonstration. Par récurrence sur n. □

Théorème 27.15 (Théorème de la base orthonormée incomplète)**.** *E un espace euclidien. Tout système orthonormé de p vecteurs de E peut être complété en une base orthonormée de E.*

Démonstration. Par récurrence descendante. $\mathcal{H}(p)$: Tout système orthonormé de p vecteurs de E peut être complété en une base orthonormée de E. $\mathcal{H}(\dim E)$ est vraie. Supposer $\mathcal{H}(p)$ vraie pour $p\in[\![1,\dim E]\!]$. Soit $(x_1,\dots,x_{p-1})$ un système orthonormé de $(p-1)$ vecteurs de E. Montrer que $\mathrm{Vect}(x_1,\dots,x_{p-1})\neq E$ et choisir $x\in E\setminus \mathrm{Vect}(x_1,\dots,x_{p-1})$. Poser alors $y = x - \sum_{i=1}^n \langle x, x_i\rangle\, x_i$ puis $x_p = \frac{y}{\|y\|}$. Vérifier que $(x_1,\dots,x_p)$ est un système orthonormé et le compléter en une base orthonormée avec $\mathcal{H}(p)$; en déduire $\mathcal{H}(p-1)$. □

Corollaire 27.16. *Tout espace euclidien non nul admet une base orthonormée.*

Proposition 27.17. *E un espace euclidien. $e=(e_1,\dots,e_n)$ une base orthonormée de E. $(x,y)\in E^2$.*

(i) $x = \sum_{i=1}^n \langle x, e_i\rangle\, e_i$,

(ii) $\langle x, y\rangle = \sum_{i=1}^n (\langle x, e_i\rangle \cdot \langle y, e_i\rangle)$,

(iii) $\langle x, y\rangle = {}^tXY = {}^tYX$, *avec* $X = Mat_e(x)$, $Y = Mat_e(y)$.

II.2 Orthogonal d'une partie

Proposition 27.18. *E un espace préhilbertien. $A\subset E$, $B\subset E$, F sous-espace vectoriel de E de dimension finie.*

(i) $A^\perp$ *est un sous-espace vectoriel de E.*

(ii) $A^\perp = (\mathrm{Vect}(A))^\perp$.

(iii) $\mathrm{Vect}(A)\subset \left(A^\perp\right)^\perp$.

(iv) $\mathrm{Vect}(A)$ *et* $A^\perp$ *sont en somme directe.*

(v) $A\subset B \Longrightarrow B^\perp\subset A^\perp$.

(vi) $\{0\}^\perp = E$ *et* $E^\perp = \{0\}$.

(vii) $F^\perp$ *est l'ensemble des vecteurs orthogonaux à tous les vecteurs d'une base de F.*

Notation 27.19. *E un espace préhilbertien. Si deux sous-espaces vectoriels F et G de E sont supplémentaires et orthogonaux, on notera $E = F \overset{\perp}{\oplus} G$.*

Proposition 27.20. *E un espace préhilbertien. F un sous-espace vectoriel de E admettant un supplémentaire orthogonal G : $E = F \overset{\perp}{\oplus} G$. Alors $\left(F^\perp\right)^\perp = F$.*

Proposition 27.21. *E un espace préhilbertien. F un sous-espace vectoriel de E de dimension finie.*

(i) $E = F \oplus F^\perp$.

(ii) $\left(F^\perp\right)^\perp = F$.

Définition 27.22 (Projection orthogonale)**.** *E un espace préhilbertien. F et G deux sous-espaces vectoriels de E t.q. $E = F \overset{\perp}{\oplus} G$. On appelle* projection orthogonale *sur F, notée p_F, la projection sur F parallèlement à G.*

Proposition 27.23. *E un espace préhilbertien. F un sous-espace vectoriel de E de dimension finie, de base orthonormée $(e_1, \dots, e_p)$, p_F la projection orthogonale sur F (qui existe car $E = F \oplus F^\perp$). Alors*

$$\forall x \in E,\ p_F(x) = \sum_{i=1}^{p} \langle x, e_i \rangle\, e_i.$$

Définition 27.24 (Distance)**.** *E un espace préhilbertien. $A \subset E$, $A \neq \varnothing$. $x \in E$. On appelle distance de x à A :*

$$d(x, A) = \inf_{a \in A} \|x - a\|.$$

Proposition 27.25. *E un espace préhilbertien. F un sous-espace vectoriel de E de dimension finie, p_F la projection orthogonale sur F. $x \in E$. Alors la distance de x à F est atteinte en un unique point de F qui est $p_F(x)$, et on a :*

$$(d(x, F))^2 = \|x - p_F(x)\|^2 = \|x\|^2 - \|p_F(x)\|^2.$$

Vocabulaire 27.26 (Vecteur normal)**.** *E un espace euclidien. H un hyperplan de E. Tout vecteur de $H^\perp$ est dit* vecteur normal *à H.*

Proposition 27.27. *E un espace euclidien. H un hyperplan de E. Soit n un vecteur unitaire (i.e. $\|n\| = 1$) normal à H. Alors*

$$\forall x \in E,\ d(x, H) = |\langle x, n \rangle|.$$

Définition 27.28. *E un espace euclidien. $\mathscr{H}$ un hyperplan affine de E. On définit la projection affine orthogonale sur $\mathscr{H}$, notée $p_{\mathscr{H}}$ par, pour $M \in E$, $p_{\mathscr{H}}(M) = M'$, où $M' \in \mathscr{H}$ et $\overrightarrow{M'M} \in \mathscr{H}^\perp$.*

Proposition 27.29. *E un espace euclidien. $\mathscr{H} = M_0 + H$ un hyperplan affine de E, où $M_0 \in E$, H hyperplan de E. n un vecteur unitaire normal à H. Alors*

$$\forall M \in E,\ d(M, \mathscr{H}) = \left|\left\langle \overrightarrow{M_0 M}, n \right\rangle\right|.$$

Vocabulaire 27.30 (Endomorphisme symétrique)**.** *E un espace préhilbertien. $u \in \mathcal{L}(E)$ est dit* endomorphisme symétrique *lorsque*

$$\forall (x, y) \in E^2,\ \langle u(x), y \rangle = \langle x, u(y) \rangle.$$

Proposition 27.31. *E un espace euclidien. $p \in \mathcal{L}(E)$ un projecteur. Alors p est un projecteur orthogonal* ssi *p est symétrique.*

Proposition 27.32. *E un espace euclidien, ε une base orthonormée de E. $u \in \mathcal{L}(E)$. Alors u est symétrique* ssi $\mathrm{Mat}_\varepsilon(u) \in \mathscr{S}_n(\mathbb{R})$.

Corollaire 27.33. *E un espace euclidien, ε une base orthonormée de E. $p \in \mathcal{L}(E)$. Alors p est un projecteur orthogonal* ssi $\mathrm{Mat}_\varepsilon(p) = {}^t(\mathrm{Mat}_\varepsilon(p)) = (\mathrm{Mat}_\varepsilon(p))^2$.

II.3 Inégalité de Bessel et conséquences

Proposition 27.34 (Inégalité de Bessel)**.** *E un espace préhilbertien. F un sous-espace vectoriel de E de dimension finie, de base orthonormée $(e_1, \dots, e_n)$, p_F la projection orthogonale sur F. Alors*

$$\forall x \in E,\ \|p_F(x)\|^2 = \sum_{i=1}^{n} \langle x, e_i\rangle^2 \leqslant \|x\|^2 .$$

Définition 27.35 (Convergence vectorielle)**.** *E un espace préhilbertien. $(x_p) \in E^{\mathbb{N}}$. On dit que $x_p \xrightarrow[p\to+\infty]{} x \in E$ lorsque $\|x_p - x\| \xrightarrow[p\to+\infty]{} 0$.*

Définition 27.36 (Suite totale)**.** *E un espace préhilbertien. $(e_i) \in E^{\mathbb{N}}$. On dit que la suite (e_i) est* totale *lorsque*

$$\forall x \in E,\ \exists (x_p) \in (\mathrm{Vect}(e_i,\ i \in \mathbb{N}))^{\mathbb{N}},\ x_p \xrightarrow[p\to+\infty]{} x.$$

Proposition 27.37. *E un espace préhilbertien. $(e_i) \in E^{\mathbb{N}}$ une suite de vecteurs orthonormés, totale dans E. Pour $n \in \mathbb{N}$, on note $F_n = \mathrm{Vect}(e_0, \dots, e_n)$ et p_n la projection orthogonale sur F_n. Alors*

$$\forall x \in E,\ p_n(x) \xrightarrow[n\to+\infty]{} x.$$

Démonstration. Utiliser l'inégalité de Bessel pour montrer que la suite $\left(\|p_n(x)\|^2\right)$ est majorée par $\|x\|^2$; comme elle est croissante en déduire que $\|p_n(x)\|^2 \xrightarrow[n\to+\infty]{} \ell \in \left[0, \|x\|^2\right]$. Supposer par l'absurde que $\ell < \|x\|^2$. Montrer que $\forall y \in \mathrm{Vect}(e_i,\ i \in \mathbb{N})$, $\|x - y\|^2 \geqslant \|x\|^2 - \ell > 0$. Ceci contredit le fait que (e_i) est totale. En déduire que $\|x - p_n(x)\|^2 = \|x\|^2 - \|p_n(x)\|^2 \xrightarrow[n\to+\infty]{} 0$. □

II.4 Procédé de Gram-Schmidt

Proposition 27.38 (Procédé de Gram-Schmidt)**.** *E un espace préhilbertien. $(v_1, \dots, v_n)$ une famille libre de E. Alors il existe une unique famille orthonormée $(w_1, \dots, w_n)$ de E t.q. $\forall i \in [\![1, n]\!]$, $\mathrm{Vect}(v_1, \dots, v_i) = \mathrm{Vect}(w_1, \dots, w_i)$ et $\forall i \in [\![1, n]\!]$, $\langle w_i, v_i\rangle > 0$.*

Démonstration. On notera $F_i = \mathrm{Vect}(v_1, \dots, v_i)$ pour $i \in [\![1, n]\!]$ et $F_0 = \{0\}$. *Analyse.* Supposer que $w_1, \dots, w_n$ existent. Pour $i \in [\![1, n]\!]$, $(w_1, \dots, w_i)$ est une base orthonormée de F_i et $v_i \in F_i$, donc $v_i = \sum_{k=1}^{i} \langle v_i, w_k\rangle w_k$, donc $v_i - p_{F_{i-1}}(v_i) = \langle v_i, w_i\rangle w_i$, où $p_{F_{i-1}}$ est la projection orthogonale sur F_{i-1}. En notant $x_i = v_i - p_{F_{i-1}}(v_i)$ ($x_i \neq 0$ car $(v_1, \dots, v_n)$ est libre), on a w_i colinéaire à x_i, et w_i unitaire, donc $w_i = \pm\frac{x_i}{\|x_i\|}$. Vérifier que $\langle x_i, v_i\rangle = \|x_i\|^2 > 0$, et en déduire que $w_i = +\frac{x_i}{\|x_i\|}$. *Synthèse.* Vérifier que $w_1, \dots, w_n$ conviennent. □

Corollaire 27.39. *E un espace euclidien. $(e_1, \dots, e_n)$ une base de E. Alors E admet une unique base orthonormée $(w_1, \dots, w_n)$ t.q. $\forall i \in [\![1, n]\!]$, $\mathrm{Vect}(e_1, \dots, e_i) = \mathrm{Vect}(w_1, \dots, w_i)$ et $\forall i \in [\![1, n]\!]$, $\langle w_i, e_i \rangle > 0$.*

Proposition 27.40. *E un espace euclidien. e une base de E et w la base orthonormée de E obtenue à partir de e par le procédé de Gram-Schmidt. Alors P_e^w est une matrice triangulaire supérieure d'éléments diagonaux strictement positifs.*

II.5 Polynômes orthogonaux

Proposition 27.41. *$E = \mathcal{C}^0([a, b], \mathbb{R})$. $\varphi \in E$, $\varphi > 0$. Pour $(f, g) \in E^2$, on pose $\langle f, g \rangle = \int_a^b \varphi f g$.*

(i) *$\langle \cdot, \cdot \rangle$ est un produit scalaire sur E.*

(ii) *Il existe une unique famille orthogonale de polynômes unitaires (i.e. de coefficient dominant 1) $(P_n)_{n\in\mathbb{N}}$ t.q. $\forall n \in \mathbb{N}$, $\deg P_n = n$. On dit que $(P_n)_{n\in\mathbb{N}}$ est une* famille de polynômes orthogonaux.

Démonstration. *Existence.* Par le procédé de Gram-Schmidt, il existe, pour $n \in \mathbb{N}$, $(Q_k)_{k\in[\![0,n]\!]}$ base orthonormée de $\mathbb{R}_n[X]$ t.q. $\forall k \in [\![0, n]\!]$, $\deg Q_k \leqslant k$ et $\left\langle Q_k, X^k \right\rangle > 0$. Notons que $\forall k \in \mathbb{N}$, $\deg Q_k = k$ (sinon $Q_k \in \mathbb{R}_{k-1}[X]$). Poser alors, pour $k \in \mathbb{N}$, $P_k = Q_k^*$, et vérifier que $(P_k)_{k\in\mathbb{N}}$ convient. *Unicité.* Soit $(T_k)_{k\in\mathbb{N}}$ vérifiant les mêmes propriétés que $(P_k)_{k\in\mathbb{N}}$. Soit $k \in \mathbb{N}$. Montrer que $T_k \in \mathbb{R}_k[X] \cap \mathbb{R}_{k-1}[X]^\perp$. En déduire, comme $\dim\left(\mathbb{R}_k[X] \cap \mathbb{R}_{k-1}[X]^\perp\right) = 1$, que T_k est colinéaire à P_k. Comme T_k et P_k sont unitaires, il vient $T_k = P_k$, d'où le résultat. □

Proposition 27.42. *$E = \mathcal{C}^0([a, b], \mathbb{R})$. $\varphi \in E$, $\varphi > 0$. Pour $(f, g) \in E^2$, on pose $\langle f, g \rangle = \int_a^b \varphi f g$. Alors l'unique famille $(P_n)_{n\in\mathbb{N}}$ de polynômes orthogonaux de E est totale.*

Démonstration. Appliquer le théorème de Weierstrass (théorème 26.29). □

III Orientation

Définition 27.43 (Orientation d'un espace)**.** *E un espace euclidien. On définit sur l'ensemble des bases de E la relation d'équivalence $\mathcal{R}$ par $e\mathcal{R}f \iff \det P_e^f > 0$. $\mathcal{R}$ a deux classes d'équivalence.* Orienter *l'espace E, c'est choisir une base e de E dite directe : toutes les bases f t.q. $e\mathcal{R}f$ sont dites* directes*, les autres sont dites* indirectes*.*

Proposition 27.44. *E un espace euclidien orienté. Toute famille orthonormale de p vecteurs de E, avec $p < \dim E$, peut être complétée en une base orthonormée directe de E.*

Définition 27.45 (Produit mixte)**.** *E un espace euclidien orienté de dimension n, e une base orthonormée directe de E. On définit le* produit mixte *de n vecteurs $v_1, \dots, v_n$ de E par*

$$[v_1, \dots, v_n] = \det_e(v_1, \dots, v_n).$$

Proposition 27.46. *E un espace euclidien orienté de dimension n. Alors*

$$\forall (v_1, \dots, v_n) \in E^n,\ |[v_1, \dots, v_n]| \leqslant \prod_{i=1}^{n} \|v_i\|,$$

avec égalité, pour $(v_1, \dots, v_n)$ libre ssi *la famille $(v_1, \dots, v_n)$ est orthogonale.*

Démonstration. En supposant $(v_1, \dots, v_n)$ libre, poser w la base orthonormée de E obtenue à partir de $(v_1, \dots, v_n)$ par le procédé de Gram-Schmidt. Écrire $|[v_1, \dots, v_n]| = |\det P_w^v| = \prod_{i=1}^n |\langle v_i, w_i \rangle|$, car P_w^v est triangulaire supérieure de coefficients diagonaux $\langle v_i, w_i \rangle$. Appliquer ensuite l'inégalité de Cauchy-Schwarz. □

IV Isométries

IV.1 Généralités

Définition 27.47 (Isométrie)**.** *E un espace préhilbertien. $f \in \mathcal{L}(E)$ est dit* endomorphisme orthogonal *ou* isométrie *lorsque* $\forall x \in E,\ \|f(x)\| = \|x\|$.

Proposition 27.48. *E un espace préhilbertien. $f \in \mathcal{L}(E)$ est une isométrie* ssi *f conserve le produit scalaire :* $\forall (x, y) \in E^2,\ \langle f(x), f(y) \rangle = \langle x, y \rangle$.

Proposition 27.49. *E un espace euclidien. $f \in \mathcal{L}(E)$. Les propriétés suivantes sont équivalentes :*

(i) *f est une isométrie.*

(ii) *f transforme une base orthonormée de E en une base orthonormée.*

(iii) *f transforme toute base orthonormée de E en une base orthonormée.*

Notation 27.50. *E un espace préhilbertien. On note $O(E)$ l'ensemble des isométries de E.*

Proposition 27.51. *E un espace euclidien. Alors $(O(E), \circ)$ est un groupe.*

IV.2 Matrices orthogonales

Définition 27.52 (Matrice orthogonale)**.** *$A \in \mathbb{M}_n(\mathbb{R})$. A est dite* matrice orthogonale *lorsque ${}^tAA = I_n$.*

Notation 27.53. *On note $O_n(\mathbb{R})$ l'ensemble des matrices orthogonales de $\mathbb{M}_n(\mathbb{R})$.*

Proposition 27.54. *$(O_n(\mathbb{R}), \times)$ est un groupe.*

Proposition 27.55. *$A \in \mathbb{M}_n(\mathbb{R})$. Les propriétés suivantes sont équivalentes :*

(i) *$A \in O_n(\mathbb{R})$.*

(ii) *Les vecteurs colonnes de A forment une base orthonormée de $\mathbb{R}^n$ avec le produit scalaire canonique.*

(iii) *Les vecteurs lignes de A forment une base orthonormée de $\mathbb{R}^n$ avec le produit scalaire canonique.*

Proposition 27.56. *E un espace euclidien. $\mathcal{B}$ une base orthonormée de E, $\mathcal{B}'$ une base de E. Alors $\mathcal{B}'$ est orthonormée* ssi *$P_{\mathcal{B}}^{\mathcal{B}'} \in O_n(\mathbb{R})$.*

Proposition 27.57. *E un espace euclidien. e une base orthonormée de E. $f \in \mathcal{L}(E)$.*

$$f \in O(E) \iff \mathrm{Mat}_e(f) \in O_n(\mathbb{R}).$$

Proposition 27.58. *E un espace euclidien.*

(i) $\forall A \in O_n(\mathbb{R}),\ \det A \in \{-1, 1\}$.

(ii) *L'application* $\begin{vmatrix} O(E) \longrightarrow \{-1,1\} \\ u \longmapsto \operatorname{Det} u \end{vmatrix}$ *est un morphisme de groupes.*

Notation 27.59. *E un espace euclidien. On note :*

(i) $SO(E) = \{f \in O(E),\ \operatorname{Det} f = 1\}$,

(ii) $O^-(E) = \{f \in O(E),\ \operatorname{Det} f = -1\}$,

(iii) $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}),\ \det A = 1\}$,

(iv) $O_n^-(\mathbb{R}) = \{A \in O_n(\mathbb{R}),\ \det A = -1\}$.

Les éléments de $SO(E)$ sont dits isométries directes.

Proposition 27.60. *E un espace euclidien. Alors $(SO(E), \circ)$ et $(SO_n(\mathbb{R}), \times)$ sont des groupes.*

Proposition 27.61. *E un espace euclidien. $f \in \mathcal{L}(E)$. Les propriétés suivantes sont équivalentes :*

(i) *f est une isométrie directe.*

(ii) *f transforme une base orthonormée directe de E en une base orthonormée directe.*

(iii) *f transforme toute base orthonormée directe de E en une base orthonormée directe.*

IV.3 Stabilité et isométries

Proposition 27.62. *E un espace euclidien, F un sous-espace vectoriel de E. $u \in O(E)$. Alors :*

$$u(F) \subset F \Longrightarrow u\left(F^\perp\right) \subset F^\perp.$$

Démonstration. Poser $v : \begin{vmatrix} F \longrightarrow F \\ x \longmapsto u(x) \end{vmatrix}$. Noter que $v \in O(F)$, donc en particulier v est bijectif. En déduire que $\forall x \in F^\perp,\ \forall y \in F,\ u(x) \perp y$. □

Théorème 27.63. *E un espace vectoriel de dimension finie. $u \in \mathcal{L}(E)$. Alors il existe un sous-espace vectoriel de E stable par u et de dimension 1 ou 2.*

Démonstration. On cherche $x \in E\backslash\{0\}$ t.q. $u^2(x) \in \operatorname{Vect}(x, u(x))$. Autrement dit, on cherche $P \in \mathbb{R}_2[X]$ t.q. $\operatorname{Ker} P(u) \neq \{0\}$. Or, on sait que u admet un polynôme minimal annulateur $\Pi_u \in \mathbb{R}[X]$ avec $\deg \Pi_u \geqslant 1$ (voir proposition 20.16). Soit alors P un facteur irréductible de Π_u : $\exists Q \in \mathbb{R}[X]$, $\Pi_u = PQ$. Si $P(u)$ était inversible, Q annulerait u avec $\deg Q < \deg \Pi_u$: c'est impossible ! Donc $\operatorname{Ker} P(u) \neq \{0\}$ et $\deg P \in \{1, 2\}$ car P est un irréductible de $\mathbb{R}[X]$. □

V Isométries en dimensions 2, 3 et n

V.1 Isométries en dimension 2

Notation 27.64. *Pour $\theta \in \mathbb{R}$, on note :*

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \text{et} \qquad S(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Proposition 27.65.

(i) $SO_2(\mathbb{R}) = \{R(\theta),\ \theta \in \mathbb{R}\}$,

(ii) $O_2^-(\mathbb{R}) = \{S(\theta),\ \theta \in \mathbb{R}\}$.

Proposition 27.66. *Soit* $(\theta, \varphi) \in \mathbb{R}^2$.

(i) $R(\theta)R(\varphi) = R(\theta + \varphi)$,

(ii) $R(\theta)S(\varphi) = S(\theta + \varphi)$,

(iii) $R(\theta)^{-1} = R(-\theta)$.

Proposition 27.67. *E un plan euclidien orienté. $u \in O(E)$.*

(i) *Si $u \in SO(E)$, alors il existe une base orthonormée directe ε et un $\theta \in \mathbb{R}$ t.q. $\mathrm{Mat}_\varepsilon(u) = R(\theta)$. Dans ce cas, θ est indépendant de la base choisie. On dit alors que u est la* rotation d'angle θ.

(ii) *Si $u \in O^-(E)$, alors u est une* symétrie orthogonale *par rapport à une droite.*

Proposition 27.68. $\begin{vmatrix} \mathbb{U} \longrightarrow SO_2(\mathbb{R}) \\ e^{i\theta} \longmapsto R(\theta) \end{vmatrix}$ *est un isomorphisme de groupes.*

Définition 27.69 (Angle de deux vecteurs)**.** *E un plan euclidien orienté. $(x, y) \in (E\backslash\{0\})^2$. Alors il existe une unique rotation r t.q. $r\left(\frac{x}{\|x\|}\right) = \frac{y}{\|y\|}$. On appelle* angle orienté $\widehat{(x, y)}$ *l'angle de la rotation r.*

Proposition 27.70. *E un plan euclidien orienté. $(x, y) \in (E\backslash\{0\})^2$, $\theta = \widehat{(x, y)}$. Alors on a :*

$$\langle x, y\rangle = \|x\| \cdot \|y\| \cdot \cos\theta, \tag{i}$$

$$[x, y] = \|x\| \cdot \|y\| \cdot \sin\theta. \tag{ii}$$

V.2 Isométries en dimension n

Proposition 27.71. *E un espace euclidien de dimension n. $u \in O(E)$. Alors il existe une base orthonormée ε de E t.q. $\mathrm{Mat}_\varepsilon(u)$ est diagonale par blocs de taille 1 ou 2. Les blocs de taille 1 sont égaux à ± 1, et les blocs de taille 2 sont du type $R(\theta)$, avec $\theta \in \mathbb{R}$.*

Démonstration. Par récurrence forte sur n en utilisant la proposition 27.62 et le théorème 27.63. □

V.3 Isométries en dimension 3

Proposition 27.72. *E un espace euclidien orienté de dimension 3. $u \in SO(E)$. Il existe $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon_3)$ base orthonormée directe de E et $\theta \in \mathbb{R}$ t.q.*

$$\mathrm{Mat}_\varepsilon(u) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & & \\ 0 & & R(\theta) \end{pmatrix}.$$

Pour ε_1 fixé, θ est indépendant du choix de ε_2 et ε_3. On dit alors que u est la rotation d'angle θ et d'axe $\mathrm{Vect}(\varepsilon_1)$.

Vocabulaire 27.73 (Retournement)**.** *E un espace euclidien de dimension 3. $\mathcal{D}$ une droite vectorielle de E. On appelle* retournement *d'axe $\mathcal{D}$ toute symétrie orthogonale de base $\mathcal{D}$.*

Proposition 27.74. *E un espace euclidien de dimension 3. $\mathcal{P}$ un plan vectoriel de E. Alors la symétrie orthogonale de base $\mathcal{P}$ est une isométrie indirecte.*

Chapitre 28

Dénombrement

I Ensembles finis

Vocabulaire 28.1 (Ensembles équipotents)**.** *Deux ensembles E et F sont dits* équipotents *lorsqu'il existe une bijection $E \to F$.*

Théorème 28.2. $(n,p) \in (\mathbb{N}^*)^2$.

(i) *S'il existe une injection $[\![1,p]\!] \to [\![1,n]\!]$, alors $p \leqslant n$.*

(ii) *S'il existe une surjection $[\![1,p]\!] \to [\![1,n]\!]$, alors $p \geqslant n$.*

(iii) *S'il existe une bijection $[\![1,p]\!] \to [\![1,n]\!]$, alors $p = n$.*

Démonstration. (i) Par récurrence sur p. (ii) À partir d'une surjection $[\![1,p]\!] \to [\![1,n]\!]$, construire une injection $[\![1,n]\!] \to [\![1,p]\!]$. □

Définition 28.3 (Cardinal)**.** *E un ensemble. S'il existe un $n \in \mathbb{N}^*$ et une bijection $[\![1,n]\!] \to E$, alors n est unique et n est dit* cardinal *de E, noté* $\operatorname{card} E$ *ou $|E|$. Le seul ensemble de cardinal nul est $\varnothing$. Dans ces deux cas, E est dit* fini*.*

Proposition 28.4. *E un ensemble, $a \in E$. Alors E est fini* ssi *$E \backslash \{a\}$ est fini. Dans ce cas, on a $|E \backslash \{a\}| = |E| - 1$.*

Proposition 28.5. *Les parties de $\mathbb{N}$ non vides et majorées sont exactement les parties de $\mathbb{N}$ non vides et finies.*

Proposition 28.6. *P une partie non vide et finie de $\mathbb{N}$, de cardinal n. Alors il existe une unique application strictement croissante $[\![1,n]\!] \to P$.*

Proposition 28.7. *E, F deux ensembles, $E' \subset E$.*

(i) *Si E et F sont équipotents et E est fini, alors F est fini et $|E| = |F|$.*

(ii) *Si E est fini alors E' est fini et $|E'| \leqslant |E|$, avec égalité* ssi *$E' = E$.*

(iii) *Toute intersection d'ensembles finis est finie.*

(iv) *S'il existe une injection $E \to F$ avec F fini alors E est fini et $|E| \leqslant |F|$.*

II Généralités sur les cardinaux

II.1 Premières propriétés

Lemme 28.8. *E un ensemble. $A \subset E$. Alors*

$$|A| = \sum_{x \in A} 1 = \sum_{x \in E} \mathbb{1}_A(x).$$

Proposition 28.9. *E un ensemble. $A, B \subset E$. Alors $A \cup B$ est fini et*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Lemme 28.10. *$E_1, \dots, E_p$ p ensembles finis deux à deux disjoints. Alors $\left|\bigcup_{i=1}^{p} E_i\right| = \sum_{i=1}^{p} |E_i|$.*

Proposition 28.11.

(i) *Toute réunion de p sous-ensembles finis $E_1, \dots, E_p$ d'un ensemble E est finie et :*

$$\left|\bigcup_{i=1}^{p} E_i\right| \leqslant \sum_{i=1}^{p} |E_i|.$$

(ii) *Soit $(A_i)_{i \in I}$ une partition d'un ensemble fini E, avec $\forall (i,j) \in I^2$, $i \neq j \Rightarrow A_i \neq A_j$. Alors I est fini et*

$$|E| = \sum_{i \in I} |A_i|.$$

II.2 Applications et cardinal

Proposition 28.12. *E, F deux ensembles finis t.q. $|E| = |F|$. $f : E \to F$. Alors f est injective* ssi *f est surjective* ssi *f est bijective.*

Proposition 28.13. *E un ensemble fini, F un ensemble quelconque. $f : E \to F$. Alors $f(E)$ est fini et $|f(E)| \leqslant |E|$, avec égalité* ssi *f est injective.*

Lemme 28.14 (Lemme des bergers)**.** *E un ensemble fini, F un ensemble quelconque. $f : E \to F$. Si $\exists p \in \mathbb{N}^*$, $\forall y \in F$, $\left|f^{-1}(\{y\})\right| = p$, alors $|E| = p|F|$.*

Démonstration. Écrire $E = \bigsqcup_{y \in F} f^{-1}(\{y\})$. □

III Arrangements et combinaisons

Notation 28.15. *Soit $(n,p) \in \mathbb{N}^2$ avec $p \leqslant n$. On note :*

(i) $A_n^p = \frac{n!}{(n-p)!}$,

(ii) $\binom{n}{p} = \frac{n!}{p!(n-p)!}$.

Proposition 28.16. *E, F deux ensembles finis. On note $p = |E|$, $n = |F|$ et on suppose $p \leqslant n$. Alors le nombre d'injections $E \to F$ est A_n^p.*

Corollaire 28.17. *E un ensemble fini de cardinal n. Alors $|\mathfrak{S}_E| = n!$.*

Vocabulaire 28.18. *E un ensemble fini de cardinal p. $q \in [\![0, p]\!]$.*

(i) *On appelle* q-liste *de E tout q-uplet d'éléments de E. L'ensemble des q-listes de E est donc E^q.*

(ii) *On appelle* arrangement *de q éléments de E toute q-liste d'éléments de E deux à deux distincts.*

(iii) *On appelle* combinaison *de q éléments de E toute partie finie à q éléments de E. On note $\mathcal{P}_q(E)$ l'ensemble des combinaisons de q éléments de E.*

Proposition 28.19. *E, F deux ensembles finis.*

(i) $|E \times F| = |E| \cdot |F|$,

(ii) $\left|F^E\right| = |F|^{|E|}$,

(iii) $|\mathcal{P}(E)| = 2^{|E|}$.

Proposition 28.20. *E un ensemble fini de cardinal p. $q \in [\![0, p]\!]$.*

(i) *Le nombre de q-listes de E est p^q.*

(ii) *Le nombre d'arrangements de q éléments de E est A_p^q.*

(iii) *Le nombre de combinaisons de q éléments de E est $\binom{p}{q}$.*

Proposition 28.21. $n \in \mathbb{N}^*$.

$$\forall k \in [\![0, n[\![,\ \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}, \tag{i}$$

$$\forall k \in [\![0, n]\!],\ \binom{n+1}{k+1} = \frac{n+1}{k+1}\binom{n}{k}, \tag{ii}$$

$$\max_{0 \leqslant k \leqslant n} \binom{n}{k} = \binom{n}{\lfloor \frac{n}{2} \rfloor}. \tag{iii}$$

Chapitre 29

Probabilités – Généralités

I Espaces probabilisables

Vocabulaire 29.1 (Expérience aléatoire)**.** *Une* expérience aléatoire *est une expérience dont on ne peut pas prédire le résultat. Pour une telle expérience, on note* Ω*, dit* univers*, l'ensemble des résultats possibles.*

Définition 29.2 (Tribu)**.** *On appelle* tribu *tout* $\mathcal{T} \subset \mathcal{P}(\Omega)$ *vérifiant les trois propriétés suivantes :*

(i) $\Omega \in \mathcal{T}$.

(ii) *Pour toute famille* $(A_i)_{i\in I}$ *d'éléments de* $\mathcal{T}$*, avec* I *fini ou dénombrable,* $\bigcup_{i\in I} A_i \in \mathcal{T}$.

(iii) *Pour tout* $A \in \mathcal{T}$, $\overline{A} \in \mathcal{T}$.

Définition 29.3 (Espace probabilisable)**.** *Si* $\mathcal{T}$ *est une tribu de* Ω*, on dit que* $(\Omega, \mathcal{T})$ *est un* espace probabilisable*.*

Remarque 29.4. *Dans le cas où* Ω *est fini, on choisira toujours* $\mathcal{T} = \mathcal{P}(\Omega)$.

Vocabulaire 29.5. $(\Omega, \mathcal{T})$ *un espace probabilisable.*

(i) *Tout élément de* $\mathcal{T}$ *est dit* événement*.*

(ii) Ω *est dit* événement certain*,* $\varnothing$ *est dit* événement impossible*.*

(iii) *Un événement* A *est dit* réalisé *si le résultat* ω *de l'expérience appartient à* A.

(iv) *L'*événement contraire *de* A *est* $\overline{A}$.

(v) *L'événement "*A et B*" est* $A \cap B$.

(vi) *L'événement "*A ou B*" est* $A \cup B$.

(vii) *On dit que* A implique B *lorsque* $A \subset B$.

(viii) *On dit que* A et B sont incompatibles *lorsque* $A \cap B = \varnothing$.

(ix) *Pour* $\omega \in \Omega$, $\{\omega\}$ *est dit* événement élémentaire*.*

(x) *On dit qu'une famille d'événements* $(A_i)_{i\in I}$ *est un* système complet d'événements *(SCE) lorsque* $\bigcup_{i\in I} A_i = \Omega$ *et* $\forall (i,j) \in I^2$, $i \neq j \Rightarrow A_i \cap A_j = \varnothing$.

Définition 29.6 (Variable aléatoire)**.** Ω *fini. Toute application* $X : \Omega \to E$*, où* E *est un ensemble quelconque, est dite* variable aléatoire*.*

Notation 29.7. Ω *fini.* $X : \Omega \to E$ *une variable aléatoire.*

(i) *Pour* $a \in E$, $(X = a)$ *est l'événement* $X^{-1}(\{a\})$.

(ii) *Pour* $F \subset E$, $(X \in F)$ *est l'événement* $X^{-1}(F)$.

(iii) *Si* $E \subset \mathbb{R}$, $(a, b) \in \mathbb{R}^2$, $(a \leqslant X \leqslant b)$ *est l'événement* $(X \in [a, b])$.

II Probabilités

II.1 Généralités

Définition 29.8 (Probabilité)**.** $(\Omega, \mathcal{T})$ *un espace probabilisable. On appelle* probabilité *toute application* $\mathbb{P} : \mathcal{T} \to [0,1]$ *vérifiant les deux propriétés suivantes :*

(i) $\mathbb{P}(\Omega) = 1$.

(ii) *Pour toute suite* $(A_i)_{i\in\mathbb{N}}$ *d'événements deux à deux incompatibles :*

$$\mathbb{P}\left(\bigcup_{i\in\mathbb{N}} A_i\right) = \sum_{i=0}^{\infty} \mathbb{P}(A_i).$$

Proposition 29.9. Ω *fini. Alors* $\mathbb{P} : \mathcal{P}(\Omega) \to [0,1]$ *est une probabilité sur* $(\Omega, \mathcal{P}(\Omega))$ ssi *les deux propriétés suivantes sont vérifiées :*

(i) $\mathbb{P}(\Omega) = 1$.

(ii) *Si* A, B *sont deux événements incompatibles :*

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B).$$

Définition 29.10 (Espace probabilisé)**.** *Si* $\mathcal{T}$ *est une tribu de* Ω *et* $\mathbb{P}$ *est une probabilité sur* $(\Omega, \mathcal{T})$*, on dit que* $(\Omega, \mathcal{T}, \mathbb{P})$ *est un* espace probabilisé*.*

Proposition 29.11. Ω *fini,* $\mathbb{P}$ *probabilité sur* $(\Omega, \mathcal{P}(\Omega))$*. Alors :*

$$\forall A \in \mathcal{P}(\Omega),\ \mathbb{P}(A) = \sum_{\omega\in A} \mathbb{P}\left(\{\omega\}\right).$$

Proposition 29.12. $\Omega = \{\omega_1, \ldots, \omega_n\}$. $(p_1, \ldots, p_n) \in \mathbb{R}^n$ *t.q.* $\forall i \in [\![1, n]\!]$, $p_i \geqslant 0$ *et* $\sum_{i=1}^n p_i = 1$*. Alors l'application* $\mathbb{P} : \mathcal{P}(\Omega) \to [0,1]$ *vérifiant* $\forall i \in [\![1, n]\!]$, $\mathbb{P}\left(\{\omega_i\}\right) = p_i$ *est une probabilité. On dit alors que* $(p_1, \ldots, p_n)$ *est une* distribution de probabilités *sur* Ω*.*

Exemple 29.13. Ω *fini. La* probabilité uniforme *sur* Ω *est la probabilité* $\mathbb{P}$ *telle que* $\forall \omega \in \Omega,\ \mathbb{P}\left(\{\omega\}\right) = \frac{1}{|\Omega|}$.

II.2 Propriétés des probabilités

Remarque 29.14. *Dans toute la suite,* Ω *est fini et on se place dans l'espace probabilisé* $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$*.*

Proposition 29.15. A, B *deux événements quelconques.* $A_1, \ldots, A_n$ *n événements quelconques.*

(i) $\mathbb{P}\left(\overline{A}\right) = 1 - \mathbb{P}(A)$,

(ii) $\mathbb{P}(\varnothing) = 0$,

(iii) $A \subset B \Longrightarrow \mathbb{P}(A) \leqslant \mathbb{P}(B)$,

(iv) $\mathbb{P}\left(A \cup B\right) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}\left(A \cap B\right)$,

(v) $\mathbb{P}\left(A \backslash B\right) = \mathbb{P}(A) - \mathbb{P}\left(A \cap B\right)$,

(vi) $\mathbb{P}\left(\bigcup_{i=1}^n A_i\right) \leqslant \sum_{i=1}^n \mathbb{P}\left(A_i\right)$.

III Probabilités conditionnelles

Définition 29.16 (Probabilité conditionnelle)**.** *A un événement t.q. $\mathbb{P}(A) > 0$. Alors l'application*

$$\mathbb{P}_A : B \in \mathcal{P}(\Omega) \longmapsto \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(A)} \in [0,1]$$

est une probabilité, dite probabilité conditionnelle sachant *A.*

Proposition 29.17 (Formule des conditionnements successifs)**.** *$A_1, \ldots, A_n$ n événements t.q. $\mathbb{P}\left(\bigcap_{i=1}^n A_i\right) > 0$. Alors :*

$$\mathbb{P}\left(\bigcap_{i=1}^n A_i\right) = \mathbb{P}(A_1) \cdot \mathbb{P}_{A_1}(A_2) \cdots \mathbb{P}_{A_1 \cap \cdots \cap A_{n-1}}(A_n).$$

Proposition 29.18 (Formule des probabilités totales)**.** *$(A_1, \ldots, A_n)$ un système complet d'événements. Γ un événement. Alors :*

$$\mathbb{P}(\Gamma) = \sum_{i=1}^n \mathbb{P}(A_i) \cdot \mathbb{P}_{A_i}(\Gamma).$$

Proposition 29.19 (Formule de Bayes)**.** *$(A_1, \ldots, A_n)$ un système complet d'événements. Γ un événement avec $\mathbb{P}(\Gamma) > 0$. Alors :*

$$\forall i \in [\![1,n]\!],\ \mathbb{P}_\Gamma(A_i) = \frac{\mathbb{P}(\Gamma \cap A_i)}{\mathbb{P}(\Gamma)} = \frac{\mathbb{P}(A_i) \cdot \mathbb{P}_{A_i}(\Gamma)}{\sum_{i=1}^n \mathbb{P}(A_i) \cdot \mathbb{P}_{A_i}(\Gamma)}.$$

IV Indépendance d'événements

IV.1 Indépendance de deux événements

Définition 29.20 (Indépendance de deux événements)**.** *Deux événements A et B sont dits* indépendants *lorsque*

$$\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot \mathbb{P}(B).$$

De plus, n événements $A_1, \ldots, A_n$ sont dits indépendants deux à deux *si pour tout $(i,j) \in [\![1,n]\!]^2$ avec $i \neq j$, A_i et A_j sont indépendants.*

Proposition 29.21. *A, B deux événements. A et B sont indépendants* ssi *$\overline{A}$ et B sont indépendants* ssi *$\overline{A}$ et $\overline{B}$ sont indépendants.*

IV.2 Indépendance mutuelle

Définition 29.22 (Indépendance mutuelle)**.** *On dit que n événements $A_1, \ldots, A_n$ sont* mutuellement indépendants *lorsque :*

$$\forall J \subset [\![1,n]\!],\ \mathbb{P}\left(\bigcap_{j \in J} A_j\right) = \prod_{j \in J} \mathbb{P}(A_j).$$

Proposition 29.23. *Si n événements sont mutuellement indépendants, alors ils sont indépendants deux à deux.*

Proposition 29.24. *$A_1, \ldots, A_n$ n événements mutuellement indépendants et $E_1, \ldots, E_n$ n événements t.q. $\forall i \in [\![1,n]\!]$, $E_i \in \left\{A_i, \overline{A_i}\right\}$. Alors $E_1, \ldots, E_n$ sont mutuellement indépendants.*

IV.3 Expériences indépendantes

Proposition 29.25. *Soit $\mathcal{E}_1, \dots, \mathcal{E}_n$ n expériences associées à des univers $\Omega_1, \dots, \Omega_n$ finis et munis de probabilités $\mathbb{P}_1, \dots, \mathbb{P}_n$. On note $\mathcal{E}$ l'expérience constituée des n expériences $\mathcal{E}_1, \dots, \mathcal{E}_n$, d'univers $\Omega = \Omega_1 \times \cdots \times \Omega_n$. On admet l'existence d'une probabilité $\mathbb{P}$ définie sur $\mathcal{P}(\Omega)$ et telle que*

$$\forall (A_1, \dots, A_n) \in \mathcal{P}(\Omega_1) \times \cdots \times \mathcal{P}(\Omega_n),\ \mathbb{P}(A_1, \dots, A_n) = \prod_{i=1}^{n} \mathbb{P}_i(A_i).$$

On dit alors que les expériences $\mathcal{E}_1, \dots, \mathcal{E}_n$ sont indépendantes *(avec la probabilité $\mathbb{P}$).*

Proposition 29.26 (Expériences de Bernoulli et loi binomiale)**.** *Une* expérience de Bernoulli *est une expérience d'univers $\Omega = \{0, 1\}$. On note p la probabilité d'obtenir 1 et $q = 1 - p$. On répète n expériences de Bernoulli indépendantes et identiques. Soit X le nombre de 1 obtenu. On a $X(\Omega) = [\![0, n]\!]$ et :*

$$\forall k \in [\![0, n]\!],\ \mathbb{P}(X = k) = \binom{n}{k} p^k q^{n-k}.$$

Chapitre 30

Variables Aléatoires Réelles

Remarque 30.1. *Dans toute la suite, Ω est fini et on se place dans l'espace probabilisé $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$.*

I Généralités

Notation 30.2. *$X : \Omega \to \mathbb{R}$ une variable aléatoire réelle.*

(i) *Pour $a \in \mathbb{R}$, $(X = a)$ est l'événement $X^{-1}(\{a\})$.*

(ii) *Pour $F \subset \mathbb{R}$, $(X \in F)$ est l'événement $X^{-1}(F)$.*

(iii) *Pour $(a, b) \in \mathbb{R}^2$, $(a \leqslant X \leqslant b)$ est l'événement $(X \in [a, b])$.*

On note $F_X : x \in \mathbb{R} \longmapsto \mathbb{P}(X \leqslant x)$, dite fonction de répartition. *Alors $\forall (a, b) \in \mathbb{R}^2$, $\mathbb{P}(a < X \leqslant b) = F_X(b) - F_X(a)$.*

Proposition 30.3 (Loi de probabilité)**.** *$X : \Omega \to E$ une variable aléatoire. Alors l'application*

$$\mathbb{P}_X : \left| \begin{array}{c} \mathcal{P}(X(\Omega)) \longrightarrow [0,1] \\ A \longmapsto \mathbb{P}(X \in A) \end{array} \right.$$

est une probabilité, dite loi de probabilité *de X.*

Notation 30.4. *$X, Y : \Omega \to E$ deux variables aléatoires. On notera $X \sim Y$ lorsque X et Y ont la même loi de probabilité.*

Exemple 30.5. *$X : \Omega \to E$ une variable aléatoire.*

(i) *On dit que $X \sim \mathcal{U}(E)$ lorsque $X(\Omega) = E$ (avec E fini non vide) et $\forall e \in E$, $\mathbb{P}(X = e) = \frac{1}{|E|}$.*

(ii) *On dit que $X \sim \mathrm{Be}(p)$ lorsque $X(\Omega) = \{0, 1\}$ et $\mathbb{P}(X = 1) = p$, $\mathbb{P}(X = 0) = 1 - p$.*

(iii) *On dit que $X \sim \mathcal{B}(n, p)$ lorsque $X(\Omega) = [\![0, n]\!]$ et $\forall k \in [\![0, n]\!]$, $\mathbb{P}(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}$.*

Proposition 30.6. *$X : \Omega \to E$ une variable aléatoire, $f : E \to F$ une application. Alors $Y = f(X)$ est une variable aléatoire $\Omega \to F$ et sa loi de probabilité est caractérisée par $Y(\Omega) = f(X(\Omega))$ et :*

$$\forall y \in X(\Omega),\ \mathbb{P}(Y = y) = \sum_{x \in f^{-1}(\{y\})} \mathbb{P}(X = k).$$

Proposition 30.7. *Si X suit une loi uniforme à valeurs réelles et $(\alpha, \beta) \in \mathbb{R}^2$, alors $\alpha X + \beta$ suit une loi uniforme.*

II Espérance et variance d'une variable aléatoire réelle

II.1 Espérance

Définition 30.8 (Espérance)**.** *$X : \Omega \to \mathbb{R}$ une variable aléatoire réelle. On définit :*

$$E(X) = \sum_{x \in X(\Omega)} x\mathbb{P}(X = x).$$

Exemple 30.9.

(i) *Si $X \sim \mathcal{U}([\![n, m]\!])$, alors $E(X) = \frac{n+m}{2}$.*

(ii) *Si $X \sim \mathrm{Be}(p)$, alors $E(X) = p$.*

(iii) *Si $X \sim \mathcal{B}(n, p)$, alors $E(X) = np$.*

Proposition 30.10. *L'espérance est linéaire. Autrement dit, si X et Y sont des variables aléatoires réelles et $(\alpha, \beta) \in \mathbb{R}^2$, alors*

$$E(\alpha X + \beta Y) = \alpha E(X) + \beta E(Y).$$

Démonstration. Soit $Z = \alpha X + \beta Y$. On note, pour $z \in Z(\Omega) : S_z = \{(x, y) \in X(\Omega) \times Y(\Omega),\ \alpha x + \beta y = z\}$. En utilisant le fait que $\bigsqcup_{z \in Z(\Omega)} S_z = X(\Omega) \times Y(\Omega)$, écrire :

$$\begin{aligned} E(Z) &= \sum_{z \in Z(\Omega)} z\mathbb{P}(Z = z) \\ &= \sum_{z \in Z(\Omega)} z \sum_{(x,y) \in S_z} \mathbb{P}\left((X = x) \cap (Y = y)\right) \end{aligned}$$

$$\begin{aligned} E(Z) &= \alpha \sum_{z \in Z(\Omega)} \sum_{(x,y) \in S_z} x\mathbb{P}\left((X = x) \cap (Y = y)\right) \\ &\quad + \beta \sum_{z \in Z(\Omega)} \sum_{(x,y) \in S_z} y\mathbb{P}\left((X = x) \cap (Y = y)\right) \\ &= \alpha \sum_{x \in X(\Omega)} x \underbrace{\sum_{y \in Y(\Omega)} \mathbb{P}\left((X = x) \cap (Y = y)\right)}_{\mathbb{P}(X=x)} \\ &\quad + \beta \sum_{y \in Y(\Omega)} y \underbrace{\sum_{x \in X(\Omega)} \mathbb{P}\left((X = x) \cap (Y = y)\right)}_{\mathbb{P}(Y=y)} \\ &= \alpha E(X) + \beta E(Y). \end{aligned}$$

□

Proposition 30.11. *$X : \Omega \to \mathbb{N}$ une variable aléatoire. Alors :*

$$E(X) = \sum_{k \in \mathbb{N}^*} \mathbb{P}(X \geqslant k).$$

Proposition 30.12. *X, Y deux variables aléatoires réelles.*

(i) *$X \geqslant 0 \Longrightarrow E(X) \geqslant 0$, avec égalité* ssi *$\mathbb{P}(X = 0) = 1$.*

(ii) *$X \geqslant Y \Longrightarrow E(X) \geqslant E(Y)$.*

II.2 Formule de transfert

Proposition 30.13 (Formule de transfert)**.** *$X : \Omega \to E$ une variable aléatoire, $f : X(\Omega) \to \mathbb{R}$ une application.*

$$E\left(f(X)\right) = \sum_{x \in X(\Omega)} f(x)\mathbb{P}(X = x).$$

II.3 Variance et moments

Définition 30.14 (Moment, variance, écart-type)**.** *X une variable aléatoire réelle.*

(i) *On appelle* moment d'ordre k *de X l'espérance de X^k.*

(ii) *On appelle* variance *de X :*

$$V(X) = E\left(\left(X - E(X)\right)^2\right).$$

(iii) *On appelle* écart-type *de X : $\sigma(X) = \sqrt{V(X)}$.*

Vocabulaire 30.15. *X une variable aléatoire réelle.*

(i) *On dit que X est* centrée *lorsque $E(X) = 0$.*

(ii) *On dit que X est* centrée réduite *lorsque $E(X) = 0$ et $\sigma(X) = 1$.*

Proposition 30.16. *X une variable aléatoire réelle.*

(i) $V(X) = E\left(X^2\right) - \left(E(X)\right)^2$.

(ii) $\forall a \in \mathbb{R}, \begin{cases} V(aX) = a^2 V(X) \\ \sigma(aX) = |a|\sigma(X) \end{cases}$.

(iii) $\forall a \in \mathbb{R}, \begin{cases} V(a + X) = V(X) \\ \sigma(a + X) = \sigma(X) \end{cases}$.

(iv) $V(X) = 0$ ssi $\mathbb{P}\left(X = E(X)\right) = 1$.

(v) *$X - E(X)$ est une variable aléatoire centrée.*

(vi) *Si $\sigma(X) \neq 0$, $\frac{X - E(X)}{\sigma(X)}$ est une variable aléatoire centrée réduite.*

Exemple 30.17.

(i) *Si $X \sim \mathrm{Be}(p)$, alors $V(X) = p(1-p)$.*

(ii) *Si $X \sim \mathcal{B}(n, p)$, alors $V(X) = np(1-p)$.*

Démonstration. (i) Utiliser le fait que $X^2 = X$ car $X(\Omega) = \{0, 1\}$. (ii) Calculer d'abord $E\left(X(X-1)\right)$, puis en déduire $V(X)$. □

II.4 Inégalités

Proposition 30.18 (Inégalité de Cauchy-Schwarz)**.** *X, Y deux variables aléatoires réelles.*

(i) $|E(X)| \leqslant E\left(|X|\right)$,

(ii) $\left(E(XY)\right)^2 \leqslant E\left(X^2\right) E\left(Y^2\right)$.

Démonstration. (ii) Montrer d'abord le résultat pour $E\left(X^2\right) = E\left(Y^2\right) = 1$ en utilisant (i) et le fait que $|XY| \leqslant \frac{1}{2}\left(X^2 + Y^2\right)$. Puis généraliser. □

Proposition 30.19 (Inégalité de Markov)**.** *X une variable aléatoire réelle positive. $a \in \mathbb{R}_+^*$. Alors :*

$$\mathbb{P}(X \geqslant a) \leqslant \frac{E(X)}{a}.$$

Démonstration. Poser $Y = \mathbb{1}_{(X \geqslant a)}$, et montrer que $E(Y) = \mathbb{P}(X \geqslant a)$ et que $X \geqslant aY$. □

Proposition 30.20 (Inégalité de Bienaymé-Tchebychev)**.** *X une variable aléatoire réelle. $\varepsilon > 0$. Alors :*

$$\mathbb{P}\left(|X - E(X)| \geqslant \varepsilon\right) \leqslant \frac{V(X)}{\varepsilon^2}.$$

III Indépendance de variables aléatoires

III.1 Indépendance de deux variables aléatoires

Définition 30.21 (Indépendance de deux variables aléatoires)**.** *$X : \Omega \to E$ et $Y : \Omega \to F$ deux variables aléatoires. On dit que X et Y sont* indépendantes *lorsque :*

$$\forall (x, y) \in X(\Omega) \times Y(\Omega),\ (X = x) \text{ et } (Y = y) \text{ sont indépendants.}$$

De plus, n variables aléatoires $X_1, \ldots, X_n$ sont dites indépendantes deux à deux *si pour tout $(i, j) \in [\![1, n]\!]^2$ avec $i \neq j$, X_i et X_j sont indépendantes.*

Proposition 30.22. *$X : \Omega \to E$ et $Y : \Omega \to F$ deux variables aléatoires indépendantes. Alors :*

$$\forall A \subset X(\Omega),\ \forall B \subset Y(\Omega),\ (X \in A) \text{ et } (Y \in B) \text{ sont indépendants.}$$

Proposition 30.23. *$X : \Omega \to E$ et $Y : \Omega \to F$ deux variables aléatoires indépendantes. Alors, pour tout $f : X(\Omega) \to E'$, $g : Y(\Omega) \to F'$, $f(X)$ et $g(Y)$ sont indépendantes.*

Démonstration. Utiliser l'indépendance de $X \in f^{-1}(\{x\})$ et de $Y \in g^{-1}(\{y\})$, pour tout $(x, y) \in f(X(\Omega)) \times g(Y(\Omega))$. □

Proposition 30.24.

(i) *Soit $X \sim \mathrm{Be}(p)$ et $Y \sim \mathrm{Be}(p')$. Alors X et Y sont indépendantes* ssi *$(X = 1)$ et $(Y = 1)$ sont indépendants.*

(ii) *Soit A et B deux événements. Alors A et B sont indépendants* ssi *$\mathbb{1}_A$ et $\mathbb{1}_B$ sont indépendants.*

Proposition 30.25. *X, Y deux variables aléatoires réelles indépendantes. Alors :*

$$E(XY) = E(X)E(Y).$$

III.2 Indépendance mutuelle

Définition 30.26 (Indépendance mutuelle)**.** *$X_1, \ldots, X_n$ n variables aléatoires. On dit que $X_1, \ldots, X_n$ sont* mutuellement indépendantes *lorsque :*

$$\forall (x_1, \ldots, x_n) \in X_1(\Omega) \times \cdots \times X_n(\Omega),\ \mathbb{P}\left(\bigcap_{i=1}^{n} (X_i = x_i)\right) = \prod_{i=1}^{n} \mathbb{P}(X_i = x_i).$$

Proposition 30.27. *$X_1, \dots, X_n$ n variables aléatoires mutuellement indépendantes. Alors $\forall (A_1, \dots, A_n) \in \mathcal{P}(X_1(\Omega)) \times \cdots \times \mathcal{P}(X_n(\Omega))$, les événements $(X_1 \in A_1), \dots, (X_n \in A_n)$ sont mutuellement indépendants.*

Démonstration. Soit $A_1 \subset X_1(\Omega), \dots, A_n \subset X_n(\Omega)$. Soit k événements quelconques parmi $(X_1 \in A_1), \dots, (X_n \in A_n)$. On suppose, quitte à renuméroter les A_i, que ces k événements sont $(X_1 \in A_1), \dots, (X_k \in A_k)$. On pose alors $A'_i = A_i$ pour $i \in [\![1, k]\!]$ et $A'_i = X_i(\Omega)$ pour $i \in]\!]k, n]\!]$. Ainsi :

$$\begin{aligned}
\mathbb{P}\left(\bigcap_{i=1}^{k}(X_i \in A_i)\right) &= \mathbb{P}\left(\bigcap_{i=1}^{n}(X_i \in A'_i)\right) \\
&= \sum_{(x_1,\dots,x_n)\in A'_1\times\cdots\times A'_n} \mathbb{P}\left((X_1 = x_1) \cap \cdots \cap (X_n = x_n)\right) \\
&= \sum_{(x_1,\dots,x_n)\in A'_1\times\cdots\times A'_n} \prod_{i=1}^{n} \mathbb{P}(X_i = x_i) = \prod_{i=1}^{n} \sum_{x_i \in A'_i} \mathbb{P}(X_i = x_i) \\
&= \prod_{i=1}^{n} \mathbb{P}(X_i \in A'_i) = \prod_{i=1}^{k} \mathbb{P}(X_i \in A_i).
\end{aligned}$$

□

Corollaire 30.28. *$X_1, \dots, X_n$ n variables aléatoires mutuellement indépendantes. Alors $\forall (x_1, \dots, x_n) \in X_1(\Omega) \times \cdots \times X_n(\Omega)$, les événements $(X_1 = x_1), \dots, (X_n = x_n)$ sont mutuellement indépendants.*

Proposition 30.29. *$X_1, \dots, X_n$ n variables aléatoires mutuellement indépendantes.*

(i) *$X_1, \dots, X_n$ sont deux à deux indépendantes.*

(ii) *Pour tout $J \subset [\![1, n]\!]$, les $(X_j)_{j\in J}$ sont indépendantes.*

(iii) *Pour tout $r \in [\![1, n[\![$, toute fonction de $X_1, \dots, X_r$ est indépendante de toute fonction de $X_{r+1}, \dots, X_n$.*

Corollaire 30.30. *$X_1, \dots, X_n$ n variables aléatoires mutuellement indépendantes. Alors :*

$$E\left(\prod_{i=1}^{n} X_i\right) = \prod_{i=1}^{n} E(X_i).$$

Démonstration. Par récurrence sur n. □

III.3 Fonctions génératrices

Définition 30.31 (Fonction génératrice)**.** *$X : \Omega \to \mathbb{N}$ une variable aléatoire. On définit la* fonction génératrice *de X par :*

$$\mathcal{G}_X : t \in \mathbb{R} \longmapsto E\left(t^X\right) \in \mathbb{R}.$$

Proposition 30.32. *$X, Y : \Omega \to \mathbb{N}$ deux variables aléatoires.*

(i) *$\forall t \in \mathbb{R}$, $\mathcal{G}_X(t) = \sum_{k\in X(\Omega)} t^k \mathbb{P}(X = k)$.*

(ii) *$\mathcal{G}_X(1) = 1$, $\mathcal{G}'_X(1) = E(X)$ et $\mathcal{G}''_X(1) = E(X(X-1))$.*

(iii) *$\forall k \in \mathbb{N}$, $\mathbb{P}(X = k) = \frac{\mathcal{G}_X^{(k)}}{k!}$.*

(iv) *Si* $\mathcal{G}_X = \mathcal{G}_Y$*, alors* $X \sim Y$*.*

(v) *Si* X *et* Y *sont indépendantes alors* $\mathcal{G}_{X+Y} = \mathcal{G}_X \mathcal{G}_Y$*.*

Exemple 30.33.

(i) *Si* $X \sim \mathrm{Be}(p)$*, alors* $\forall t \in \mathbb{R}$, $\mathcal{G}_X(t) = pt + 1 - p$*.*

(ii) *Si* $X \sim \mathcal{B}(n,p)$*, alors* $\forall t \in \mathbb{R}$, $\mathcal{G}_X(t) = (pt + 1 - p)^n$*.*

IV Couples de variables aléatoires

IV.1 Loi conjointe et lois marginales

Définition 30.34 (Loi conjointe, lois marginales et lois conditionnelles)**.** X, Y *deux variables aléatoires.*

(i) *La* loi conjointe *est la loi du couple* (X, Y)*.*

(ii) *Les* lois marginales *sont les lois de* X *et de* Y*.*

(iii) *La* loi conditionnelle *de* X *par rapport à* $Y = y_j$*, où* $y_j \in Y(\Omega)$*, est déterminée par* $X(\Omega)$ *et* $\mathbb{P}_{Y=y_j}(X = x)$*, pour* $x \in X(\Omega)$*.*

Notation 30.35. X, Y *deux variables aléatoires.* $(x, y) \in X(\Omega) \times Y(\Omega)$*. On notera :*

$$\mathbb{P}(X = x, Y = y) = \mathbb{P}\left((X = x) \cap (Y = y)\right).$$

Proposition 30.36. X, Y *deux variables aléatoires réelles.*

$$\forall s \in (X+Y)(\Omega),\ \mathbb{P}(X + Y = s) = \sum_{\substack{(x,y) \in X(\Omega) \times Y(\Omega) \\ x+y=s}} \mathbb{P}(X = x, Y = y).$$

Proposition 30.37.

(i) *Si* $X_1, \ldots, X_n$ *suivent toutes la loi* $\mathrm{Be}(p)$ *et sont mutuellement indépendantes, alors* $(X_1 + \cdots + X_n) \sim \mathcal{B}(n,p)$*.*

(ii) *Si* $X \sim \mathcal{B}(n,p)$ *et* $Y \sim \mathcal{B}(m,p)$ *et* X *et* Y *sont indépendantes, alors* $(X + Y) \sim \mathcal{B}(n+m,p)$*.*

IV.2 Covariance

Définition 30.38 (Covariance)**.** X, Y *deux variables aléatoires réelles. On définit :*

$$\mathrm{cov}(X,Y) = E\left[(X - E(X))\,(Y - E(Y))\right].$$

Proposition 30.39. X, Y *deux variables aléatoires réelles.*

(i) $\mathrm{cov}(X,X) = V(X)$*.*

(ii) $\mathrm{cov}(X,Y) = E(XY) - E(X)E(Y)$*.*

(iii) *La covariance est une forme bilinéaire, symétrique et positive.*

Proposition 30.40. X, Y *deux variables aléatoires réelles.*

$$X \text{ et } Y \text{ sont indépendantes} \Longrightarrow \mathrm{cov}(X,Y) = 0.$$

Proposition 30.41. *$X_1, \dots, X_n$ n variables aléatoires réelles.*

$$V\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} V(X_i) + 2 \sum_{1 \leqslant i < j \leqslant n} \operatorname{cov}(X_i, X_j), \tag{i}$$

$$X_1, \dots, X_n \text{ indépendantes deux à deux} \Longrightarrow V\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} V(X_i). \tag{ii}$$

Corollaire 30.42. *$X_1, \dots, X_n$ n variables aléatoires réelles deux à deux indépendantes de même loi. On note $S_n = \sum_{i=1}^{n} X_i$. Alors, pour tout $\varepsilon > 0$:*

$$\mathbb{P}\left(\left|\frac{S_n}{n} - E(X_1)\right| \leqslant \varepsilon\right) \xrightarrow[n \to +\infty]{} 0.$$

On dit que $\left(\frac{S_n}{n}\right)$ converge en probabilité *vers la variable aléatoire constante $E(X_1)$.*

Chapitre 31

Ensembles Dénombrables et Familles Sommables

I Ensembles dénombrables

Définition 31.1 (Dénombrabilité)**.** *Un ensemble E est dit* dénombrable *s'il est en bijection avec $\mathbb{N}$. De plus, E est dit* au plus dénombrable *si E est dénombrable ou fini.*

Théorème 31.2. *Soit $\mathfrak{P}$ une partie infinie de $\mathbb{N}$. Alors $\mathfrak{P}$ est dénombrable. De plus, il existe une unique bijection strictement croissante $\varphi : \mathbb{N} \to \mathfrak{P}$.*

Démonstration. Construire φ par récurrence : poser $\varphi(0) = \min \mathfrak{P}$ puis, pour $k \in \mathbb{N}$, $\varphi(k+1) = \min \mathfrak{P} \setminus \{\varphi(0), \dots, \varphi(k)\}$. Montrer que φ est strictement croissante et surjective, donc bijective. Montrer ensuite l'unicité. □

Proposition 31.3. *$\mathfrak{H}$ un ensemble.*

$$\begin{aligned} \mathfrak{H} \text{ est au plus dénombrable} &\iff \text{il existe une injection } \mathfrak{H} \to \mathbb{N} \\ &\iff \text{il existe une surjection } \mathbb{N} \to \mathfrak{H}. \end{aligned}$$

Lemme 31.4. *Pour tout $k \in \mathbb{N}^*$, $\mathbb{N}^k$ est dénombrable.*

Démonstration. En notant p_i le i-ième nombre premier, montrer que

$$\left| \begin{array}{c} \mathbb{N}^k \longrightarrow \mathbb{N} \\ (a_1, \dots, a_k) \longmapsto \displaystyle\prod_{i=1}^{k} p_i^{a_i} \end{array} \right.$$

est une injection. □

Théorème 31.5. *Tout produit fini d'ensembles au plus dénombrables est au plus dénombrable.*

Exemple 31.6.

(i) *$\mathbb{Z}$ est dénombrable.*

(ii) *$\mathbb{Q}$ est dénombrable.*

Théorème 31.7. *Toute réunion au plus dénombrable d'ensembles au plus dénombrables est au plus dénombrable.*

Démonstration. Se ramener au cas d'une famille $(B_k)_{k\in\mathbb{N}}$ d'ensembles dénombrables. Pour $k \in \mathbb{N}$, poser $f_k : B_k \to \mathbb{N}$ une injection. Montrer alors que

$$\left|\begin{array}{l} \bigcup_{k\in\mathbb{N}} B_k \longrightarrow \mathbb{N}^2 \\ \qquad b \longmapsto (k_0, f_{k_0}(b)) \qquad \text{avec } k_0 = \min\{k \in \mathbb{N},\ b \in B_k\} \end{array}\right.$$

est une injection. □

II Familles sommables de réels positifs

II.1 Définition

Définition 31.8 (Famille sommable de réels positifs)**.** *Une famille $(u_i)_{i\in I}$ de réels positifs, avec I dénombrable, est dite* sommable *lorsque*

$$\exists M \geqslant 0,\ \forall J \subset I,\ J \text{ fini},\ \sum_{j\in J} u_j \leqslant M.$$

Dans ce cas, on appelle somme de la famille $(u_i)_{i\in I}$:

$$\sum_{i\in I} u_i = \sup_{\substack{J\subset I \\ J \text{ fini}}} \left(\sum_{j\in J} u_j\right).$$

Proposition 31.9. *Toute sous-famille d'une famille sommable de réels positifs est sommable.*

II.2 Caractérisations de la sommabilité

Proposition 31.10. *$(u_i)_{i\in I}$ une famille de réels positifs. $(u_i)_{i\in I}$ est sommable de somme S* ssi

$$\forall \varepsilon > 0,\ \exists K \subset I,\ K \text{ fini},\ \forall J \subset I,\ J \text{ fini},\ K \subset J \Longrightarrow S - \varepsilon \leqslant \sum_{j\in J} u_j \leqslant S.$$

Corollaire 31.11. *$(u_i)_{i\in I}$ une famille de réels positifs. $(J_n)_{n\in\mathbb{N}}$ une famille de parties finies de I t.q. $\forall n \in \mathbb{N}$, $J_n \subset J_{n+1}$ et $I = \bigcup_{n\in\mathbb{N}} J_n$. Alors $(u_i)_{i\in I}$ est sommable* ssi *la suite $\left(\sum_{j\in J_n} u_j\right)_{n\in\mathbb{N}}$ converge. Dans ce cas :*

$$\sum_{i\in I} u_i = \lim_{n\to+\infty} \left(\sum_{j\in J_n} u_j\right).$$

Proposition 31.12. *$(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ deux familles de réels positifs. Si $\forall i \in I, 0 \leqslant u_i \leqslant v_i$ et $(v_i)_{i\in I}$ est sommable alors $(u_i)_{i\in I}$ est sommable et :*

$$\sum_{i\in I} u_i \leqslant \sum_{i\in I} v_i.$$

Proposition 31.13. *$(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ deux familles de réels positifs sommables. $\lambda \in \mathbb{R}_+$.*

(i) *$(u_i + v_i)_{i\in I}$ est sommable et :*

$$\sum_{i\in I}(u_i + v_i) = \sum_{i\in I} u_i + \sum_{i\in I} v_i.$$

(ii) $(\lambda u_i)_{i\in I}$ *est sommable et :*

$$\sum_{i\in I}(\lambda u_i) = \lambda \sum_{i\in I} u_i.$$

Démonstration. En notant $S = \sum_{i\in I} u_i + \sum_{i\in I} v_i$, montrer que :

$$\forall \varepsilon > 0,\ \exists K \subset I,\ K \text{ fini},\ \forall J \subset I,\ J \text{ fini},\ K \subset J \implies S - \varepsilon \leqslant \sum_{j\in J} u_j + \sum_{j\in J} v_j = \sum_{j\in J}(u_j + v_j) \leqslant S.$$

□

Théorème 31.14 (Théorème de sommation par paquets)**.** $(u_i)_{i\in I}$ *une famille de réels positifs.* $(I_n)_{n\in\mathbb{N}}$ *une famille de parties non vides de* I *t.q.* $I = \bigsqcup_{n\in\mathbb{N}} I_n$*. Alors* $(u_i)_{i\in I}$ *est sommable* ssi *les deux conditions suivantes sont réalisées :*

(i) *Pour tout* $n \in \mathbb{N}$, $(u_i)_{i\in I_n}$ *est sommable de somme* S_n*.*

(ii) *La série* $\sum S_n$ *converge.*

Dans ce cas :

$$\sum_{i\in I} u_i = \sum_{n=0}^{\infty} \left(\sum_{i\in I_n} u_i \right).$$

III Familles sommables de réels ou complexes

III.1 Définition

Définition 31.15 (Famille sommable de réels ou complexes)**.** *Une famille* $(a_i)_{i\in I}$ *de réels ou complexes est dite* sommable *lorsque* $(|a_i|)_{i\in I}$ *est sommable.*

Définition 31.16 (Somme d'une famille de réels ou complexes)**.** $(a_j)_{j\in I}$ *une famille d'éléments de* $\mathbb{K}$*.*

(i) $\mathbb{K} = \mathbb{R}$*.* $(a_j)_{j\in I}$ *est sommable* ssi $\left(a_j^+\right)_{j\in I}$ *et* $\left(a_j^-\right)_{j\in I}$ *le sont, où* $a_j^+ = \max(a_j, 0)$ *et* $a_j^- = \max(-a_j, 0)$*. Dans ce cas, on définit :*

$$\sum_{j\in I} a_j = \left(\sum_{j\in I} a_j^+ \right) - \left(\sum_{j\in I} a_j^- \right).$$

(ii) $\mathbb{K} = \mathbb{C}$*.* $(a_j)_{j\in I}$ *est sommable* ssi $(\Re(a_j))_{j\in I}$ *et* $(\Im(a_j))_{j\in I}$ *le sont. Dans ce cas, on définit :*

$$\sum_{j\in I} a_j = \left(\sum_{j\in I} \Re(a_j) \right) + i \left(\sum_{j\in I} \Im(a_j) \right).$$

III.2 Premières propriétés

Proposition 31.17. $(a_i)_{i\in I}$ *et* $(b_i)_{i\in I}$ *deux familles sommables d'éléments de* $\mathbb{K}$*.* $(\alpha, \beta) \in \mathbb{K}^2$*. Alors* $(\alpha a_i + \beta b_i)_{i\in I}$ *est sommable et :*

$$\sum_{i\in I} (\alpha a_i + \beta b_i) = \alpha \left(\sum_{i\in I} a_i \right) + \beta \left(\sum_{i\in I} b_i \right).$$

Proposition 31.18. *$(a_i)_{i\in I}$ une famille sommable d'éléments de $\mathbb{K}$. Alors :*

$$\left|\sum_{i\in I} a_i\right| \leqslant \sum_{i\in I} |a_i|\,.$$

Démonstration. $\mathbb{K} = \mathbb{R}$. Revenir à a_i^+ et a_i^-. $\mathbb{K} = \mathbb{C}$. Même méthode que pour la proposition 24.45. □

III.3 Calculs de sommes

Proposition 31.19. *$(a_i)_{i\in I}$ une famille sommable de complexes.*

(i) *$(I_n)_{n\in\mathbb{N}}$ une famille de parties finies de I t.q. $\forall n \in \mathbb{N}$, $I_n \subset I_{n+1}$ et $I = \bigcup_{n\in\mathbb{N}} I_n$. Alors :*

$$\sum_{i\in I} a_i = \lim_{n\to+\infty} \left(\sum_{i\in I_n} a_i\right).$$

(ii) *$(I_n)_{n\in\mathbb{N}}$ une famille de parties non vides de I t.q. $I = \bigsqcup_{n\in\mathbb{N}} I_n$. Alors pour tout $n \in \mathbb{N}$, $(a_i)_{i\in I_n}$ est sommable de somme S_n, et la série $\sum S_n$ converge. De plus :*

$$\sum_{i\in I} a_i = \sum_{n=0}^{\infty} \left(\sum_{i\in I_n} a_i\right).$$

Proposition 31.20. *$(a_i)_{i\in I}$ une famille sommable de complexes. G un ensemble dénombrable. $(I_g)_{g\in G}$ une famille de parties non vides de I t.q. $I = \bigsqcup_{g\in G} I_g$. Alors pour tout $g \in G$, $(a_i)_{i\in I_g}$ est sommable de somme S_g, et la famille $(S_g)_{g\in G}$ est sommable. De plus :*

$$\sum_{i\in I} a_i = \sum_{g\in G} \left(\sum_{i\in I_g} a_i\right).$$

Proposition 31.21. *$(a_i)_{i\in I}$ une famille sommable de complexes. $\sigma : J \to I$ une bijection. Si I et J sont dénombrables, alors $\left(a_{\sigma(j)}\right)_{j\in J}$ est sommable et :*

$$\sum_{j\in J} a_{\sigma(j)} = \sum_{i\in I} a_i.$$

IV Cas particuliers

IV.1 Familles indexées par $\mathbb{N}$ ou $\mathbb{Z}$

Proposition 31.22. *$(a_n)_{n\in I}$ une famille de complexes.*

(i) *$I = \mathbb{N}$. $(a_n)_{n\in\mathbb{N}}$ est sommable* ssi *$\sum a_n$ est absolument convergente. Dans ce cas :*

$$\sum_{n\in\mathbb{N}} a_n = \sum_{n=0}^{\infty} a_n.$$

(ii) *$I = \mathbb{Z}$. $(a_n)_{n\in\mathbb{Z}}$ est sommable* ssi *$\sum a_n$ et $\sum a_{(-n)}$ sont absolument convergentes. Dans ce cas :*

$$\sum_{n\in\mathbb{Z}} a_n = \left(\sum_{n=0}^{\infty} a_n\right) + \left(\sum_{n=1}^{\infty} a_{(-n)}\right).$$

IV.2 Familles indexées par $\mathbb{N}^2$

Proposition 31.23. *Une famille de complexes $(a_{i,j})_{(i,j)\in\mathbb{N}^2}$ est sommable* ssi

$$\exists B \geqslant 0,\ \forall n \in \mathbb{N},\ \sum_{i=0}^{n}\left(\sum_{j=0}^{n}|a_{i,j}|\right) \leqslant B.$$

Théorème 31.24 (Théorème de Fubini)**.** *Une famille de complexes $(a_{i,j})_{(i,j)\in\mathbb{N}^2}$ est sommable* ssi *pour tout $j \in \mathbb{N}$ fixé, la série $\sum_i |a_{i,j}|$ est convergente de somme S_j et $\sum_j S_j$ est convergente. Dans ce cas :*

$$\sum_{(i,j)\in\mathbb{N}^2} a_{i,j} = \sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} a_{i,j}\right) = \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} a_{i,j}\right).$$

Proposition 31.25. *$(a_{i,j})_{(i,j)\in\mathbb{N}^2}$ une famille de complexes sommable. $\sigma : \mathbb{N} \to \mathbb{N}^2$ une bijection. Alors $\sum a_{\sigma(k)}$ est absolument convergente et :*

$$\sum_{k\in\mathbb{N}} a_{\sigma(k)} = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j}.$$

Proposition 31.26. *$(a_i)_{i\in\mathbb{N}}$ et $(b_j)_{j\in\mathbb{N}}$ deux familles de complexes. Si $\sum a_i$ et $\sum b_j$ sont absolument convergentes alors $(a_i b_j)_{(i,j)\in\mathbb{N}^2}$ est sommable et :*

$$\sum_{(i,j)\in\mathbb{N}^2} a_i b_j = \left(\sum_{i\in\mathbb{N}} a_i\right)\left(\sum_{j\in\mathbb{N}} b_j\right).$$

Définition 31.27 (Produit de Cauchy)**.** *$(a_i)_{i\in\mathbb{N}}$ et $(b_j)_{j\in\mathbb{N}}$ deux familles de complexes. Le* produit de Cauchy *de $(a_i)_{i\in\mathbb{N}}$ et $(b_j)_{j\in\mathbb{N}}$ est la suite $(c_n)_{n\in\mathbb{N}}$ définie par :*

$$\forall n \in \mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=n}} a_i b_j.$$

Proposition 31.28. *$(a_i)_{i\in\mathbb{N}}$ et $(b_j)_{j\in\mathbb{N}}$ deux familles de complexes de produit de Cauchy $(c_n)_{n\in\mathbb{N}}$. Si $\sum a_i$ et $\sum b_j$ sont absolument convergentes alors $\sum c_n$ est absolument convergente et :*

$$\sum_{n\in\mathbb{N}} c_n = \left(\sum_{i\in\mathbb{N}} a_i\right)\left(\sum_{j\in\mathbb{N}} b_j\right).$$

V Retour sur l'exponentielle complexe

Proposition 31.29. $\forall x \in \mathbb{R},\ e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$.

Démonstration. Utiliser la formule de Taylor avec reste intégral (proposition 12.4) appliquée à la fonction exp. □

Proposition 31.30. $\forall x \in \mathbb{R},\ e^{ix} = \sum_{n=0}^{\infty} \frac{(ix)^n}{n!}$.

Démonstration. Utiliser la formule de Taylor avec reste intégral (proposition 12.4) appliquée aux fonctions cos et sin. □

Lemme 31.31. $\forall (z_1, z_2) \in \mathbb{C}^2$, $\left(\sum_{n=0}^{\infty} \frac{z_1^n}{n!}\right)\left(\sum_{n=0}^{\infty} \frac{z_2^n}{n!}\right) = \sum_{n=0}^{\infty} \frac{(z_1+z_2)^n}{n!}$.

Démonstration. Justifier l'absolue convergence de ces séries grâce à la proposition 31.29, puis utiliser un produit de Cauchy. □

Théorème 31.32.

$$\forall z \in \mathbb{C},\ e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

Chapitre 32

Espaces Vectoriels Normés

I Normes

I.1 Définitions

Définition 32.1 (Norme)**.** *E un $\mathbb{K}$-espace vectoriel. On dit que $\mathfrak{N} : E \to \mathbb{R}$ est une* norme *lorsque les quatre propriétés suivantes sont vérifiées :*

(i) $\forall x \in E,\ \mathfrak{N}(x) \geqslant 0$,

(ii) $\forall x \in E,\ \mathfrak{N}(x) = 0 \iff x = 0$,

(iii) $\forall x \in E,\ \forall \lambda \in \mathbb{K},\ \mathfrak{N}(\lambda x) = |\lambda| \cdot \mathfrak{N}(x)$,

(iv) $\forall (x, y) \in E^2,\ \mathfrak{N}(x + y) \leqslant \mathfrak{N}(x) + \mathfrak{N}(y)$.

Définition 32.2 (Distance)**.** *E un $\mathbb{K}$-espace vectoriel. On dit que $\mathfrak{d} : E^2 \to \mathbb{R}$ est une* distance *lorsque les quatre propriétés suivantes sont vérifiées :*

(i) $\forall (x, y) \in E^2,\ \mathfrak{d}(x, y) \geqslant 0$,

(ii) $\forall (x, y) \in E^2,\ \mathfrak{d}(x, y) = 0 \iff x = y$,

(iii) $\forall (x, y) \in E^2,\ \mathfrak{d}(x, y) = \mathfrak{d}(y, x)$,

(iv) $\forall (x, y, z) \in E^3,\ \mathfrak{d}(x, z) \leqslant \mathfrak{d}(x, y) + \mathfrak{d}(y, z)$.

Vocabulaire 32.3 (Espace vectoriel normé)**.** *Un espace vectoriel est dit* normé *s'il est muni d'une norme.*

I.2 Exemples de normes

Notation 32.4. *$p \in [\![1, +\infty[\![$. On définit $\|\cdot\|_p$ sur $\mathbb{K}^n$ par :*

$$\forall x = (x_1, \ldots, x_n) \in \mathbb{K}^n,\ \|x\|_p = \sqrt[p]{\sum_{i=1}^{n} |x_i|^p}.$$

On définit aussi $\|\cdot\|_\infty$ sur $\mathbb{K}^n$ par :

$$\forall x = (x_1, \ldots, x_n) \in \mathbb{K}^n,\ \|x\|_\infty = \sup_{1 \leqslant i \leqslant n} |x_i|.$$

Lemme 32.5. *$x = (x_1, \ldots, x_n) \in \mathbb{K}^n$, $y = (y_1, \ldots, y_n) \in \mathbb{K}^n$. $(p, q) \in (\mathbb{N}^*)^2$ t.q. $\frac{1}{p} + \frac{1}{q} = 1$. Alors :*

$$\sum_{i=1}^{n} |x_i y_i| \leqslant \|x\|_p \cdot \|y\|_q.$$

Démonstration. *Première étape.* Par concavité de ln : $\forall (a,b) \in \left(\mathbb{R}_+^*\right)^2, \ln(ab) = \frac{1}{p}\ln(a^p) + \frac{1}{q}\ln(b^q) \leqslant \ln\left(\frac{a^p}{p} + \frac{b^q}{q}\right)$. Donc $\forall (a,b) \in (\mathbb{R}_+)^2, ab \leqslant \frac{a^p}{p} + \frac{b^q}{q}$. *Deuxième étape.* On suppose d'abord $\|x\|_p = 1$ et $\|y\|_q = 1$. Montrer alors que $\sum_{i=1}^n |x_i y_i| \leqslant 1$. *Troisième étape.* Se ramener au cas où $\|x\|_p = 1$ et $\|y\|_q = 1$. □

Proposition 32.6. *$\|\cdot\|_p$ et $\|\cdot\|_\infty$ sont des normes sur $\mathbb{K}^n$.*

Démonstration. $\|\cdot\|_p$ vérifie l'inégalité triangulaire car, en notant $q = \frac{p}{p-1}$, on a, pour $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$, $y = (y_1, \ldots, y_n) \in \mathbb{K}^n$:

$$\begin{aligned}\|x+y\|_p^p &\leqslant \sum_{i=1}^n |x_i| \cdot |x_i + y_i|^{p-1} + \sum_{i=1}^n |y_i| \cdot |x_i + y_i|^{p-1} \\ &\leqslant \|x\|_p \sqrt[q]{\sum_{i=1}^n |x_i + y_i|^{(p-1)q}} + \|y\|_p \sqrt[q]{\sum_{i=1}^n |x_i + y_i|^{(p-1)q}} \\ &= \|x\|_p \cdot \|x+y\|_p^{p-1} + \|y\|_p \cdot \|x+y\|_p^{p-1}.\end{aligned}$$

Les autres points sont clairs. □

Notation 32.7. *$p \in [\![1, +\infty[\![$. On définit $\|\cdot\|_p$ sur $\mathcal{C}^0([a,b], \mathbb{K})$ par :*

$$\forall f \in \mathcal{C}^0([a,b], \mathbb{K}), \ \|f\|_p = \sqrt[p]{\int_a^b |f|^p}.$$

On définit aussi $\|\cdot\|_\infty$ sur $\mathcal{C}^0([a,b], \mathbb{K})$ par :

$$\forall f \in \mathcal{C}^0([a,b], \mathbb{K}), \ \|f\|_\infty = \sup_{[a,b]} |f|.$$

Lemme 32.8. *$f, g : [a,b] \to \mathbb{K}$ $\mathcal{C}^0$. $(p,q) \in (\mathbb{N}^*)^2$ t.q. $\frac{1}{p} + \frac{1}{q} = 1$. Alors :*

$$\int_a^b |fg| \leqslant \|f\|_p \cdot \|g\|_q.$$

Proposition 32.9. *$\|\cdot\|_p$ et $\|\cdot\|_\infty$ sont des normes sur $\mathcal{C}^0([a,b], \mathbb{K})$.*

Notation 32.10. *Dans toute la suite, E est un $\mathbb{K}$-espace vectoriel et $\|\cdot\|_E$ est une norme sur E.*

I.3 Parties bornées

Définition 32.11 (Boules et sphères)**.** *$a \in E$, $r \in \mathbb{R}_+^*$. On définit :*

(i) $\mathcal{B}_o(a,r) = \{x \in E, \ \|x-a\|_E < r\}$ *(*boule ouverte*).*

(ii) $\mathcal{B}_f(a,r) = \{x \in E, \ \|x-a\|_E \leqslant r\}$ *(*boule fermée*).*

(iii) $\mathcal{S}(a,r) = \{x \in E, \ \|x-a\|_E = r\}$ *(*sphère*).*

Définition 32.12 (Partie bornée)**.** *On appelle* partie bornée *de E toute partie $X \subset E$ t.q.*

$$\exists M \geqslant 0, \ \forall x \in X, \ \|x\|_E \leqslant M.$$

Proposition 32.13. *Toute réunion finie de parties bornées est bornée.*

Définition 32.14 (Applications et suites bornées)**.**

(i) *Une application $f : A \to E$ est dite* bornée *lorsque $f(A)$ est une partie bornée de E.*

(ii) *Une suite $(u_n) \in E^{\mathbb{N}}$ est dite* bornée *lorsque $\{u_n,\ n \in \mathbb{N}\}$ est une partie bornée de E.*

Proposition 32.15. *L'ensemble $\mathcal{H} = \{f : A \to E,\ f \text{ bornée}\}$ est un $\mathbb{K}$-espace vectoriel muni de la norme $\|\cdot\|_\infty$ définie par :*

$$\forall f \in \mathcal{H},\ \|f\|_\infty = \sup_{x \in A} \|f(x)\|_E .$$

Définition 32.16 (Convergence)**.** *$(u_n) \in E^{\mathbb{N}}$. On dit que $u_n \xrightarrow[n\to+\infty]{} \ell \in E$ lorsque $\|u_n - \ell\|_E \xrightarrow[n\to+\infty]{} 0$.*

Proposition 32.17. *$(u_n) \in E^{\mathbb{N}}$, $(v_n) \in E^{\mathbb{N}}$. $(\lambda, \mu) \in \mathbb{K}^2$.*

(i) *Si (u_n) converge, alors (u_n) est bornée.*

(ii) *Si (u_n) converge, alors sa limite est unique.*

(iii) *Si (u_n) et (v_n) convergent alors $(\lambda u_n + \mu v_n)$ aussi et :*

$$\lim_{n\to+\infty} (\lambda u_n + \mu v_n) = \lambda \lim_{n\to+\infty} u_n + \mu \lim_{n\to+\infty} v_n.$$

I.4 Espace vectoriel produit

Définition 32.18 (Norme produit)**.** *$E_1, \dots, E_n$ n espaces vectoriels munis de normes respectives $\mathfrak{N}_1, \dots, \mathfrak{N}_n$. Alors l'espace $E = \prod_{i=1}^n E_i$ est un espace vectoriel normé muni de la* norme produit *définie par :*

$$\forall x = (x_1, \dots, x_n) \in E,\ \|x\|_E = \max_{1 \leqslant i \leqslant n} \mathfrak{N}_i (x_i) .$$

Proposition 32.19. *$E_1, \dots, E_n$ n espaces vectoriels munis de normes respectives $\mathfrak{N}_1, \dots, \mathfrak{N}_n$. On munit $E = \prod_{i=1}^n E_i$ de la norme produit et on note, pour $i \in [\![1, n]\!]$, $p_i : \left| \begin{array}{c} E \longrightarrow E_i \\ (x_1, \dots, x_n) \longmapsto x_i \end{array} \right.$.*

(i) *Pour $i \in [\![1, n]\!]$, p_i est linéaire, et lipschitzienne de rapport 1 :*

$$\forall x \in E,\ \mathfrak{N}_i (p_i(x)) \leqslant \|x\|_E .$$

(ii) *Pour $a \in E$, $r > 0$, on a :*

$$\mathcal{B}_o(a, r) = \prod_{i=1}^n \mathcal{B}_o (p_i(a), r) .$$

Ceci est encore vrai pour les boules fermées.

(iii) *Pour $X \subset E$, X est bornée* ssi *$\forall i \in [\![1, n]\!]$, $p_i(X)$ est bornée.*

(iv) *Pour $(u_n) \in E^{\mathbb{N}}$, $u_n \xrightarrow[n\to+\infty]{} \ell \in E$* ssi *$\forall i \in [\![1, n]\!]$, $p_i (u_n) \xrightarrow[n\to+\infty]{} p_i(\ell)$.*

II Topologie dans les espaces vectoriels normés

II.1 Voisinages, ouverts et fermés

Définition 32.20 (Voisinage, ouvert, fermé)**.**

(i) *On dit que $V \subset E$ est un* voisinage *de $a \in E$ lorsque V contient une boule ouverte centrée en a.*

(ii) *On dit que $\Omega \subset E$ est un* ouvert *lorsque Ω est un voisinage de chacun de ses points.*

(iii) *On dit que $F \subset E$ est un* fermé *lorsque $E \backslash F$ est un ouvert.*

Proposition 32.21.

(i) *Les boules ouvertes sont des ouverts.*

(ii) *Les boules fermées sont des fermés.*

Définition 32.22 (Adhérence)**.** *On dit que $x \in E$ est* adhérent *à $A \subset E$ lorsque tout voisinage de x rencontre A. On note $\overline{A}$, dit* adhérence *de A, l'ensemble des points adhérents à A.*

Proposition 32.23. *$A \subset E$, $a \in E$.*

(i) *$a \in \overline{A}$* ssi *il existe $(u_n) \in A^{\mathbb{N}}$ t.q. $u_n \xrightarrow[n\to+\infty]{} a$.*

(ii) *A est fermé* ssi *pour tout $(u_n) \in A^{\mathbb{N}}$ convergente, $(\lim_{n\to+\infty} u_n) \in A$.*

Proposition 32.24.

(i) *Une réunion quelconque d'ouverts est un ouvert.*

(ii) *Une intersection finie d'ouverts est un ouvert.*

Corollaire 32.25.

(i) *Une intersection quelconque de fermés est un fermé.*

(ii) *Une réunion finie de fermés est un fermé.*

Définition 32.26 (Intérieur)**.** *On dit que $x \in E$ est* intérieur *à $A \subset E$ lorsqu'il existe un voisinage de x inclus dans A. On note $\mathring{A}$, dit* intérieur *de A, l'ensemble des points intérieurs à A.*

Proposition 32.27. *$A \subset E$.*

(i) *$\mathring{A}$ est le plus grand ouvert inclus dans A.*

(ii) *A est ouvert* ssi *$A = \mathring{A}$.*

(iii) *$\overline{A}$ est le plus petit fermé contenant A.*

(iv) *A est fermé* ssi *$A = \overline{A}$.*

II.2 Densité

Définition 32.28 (Densité)**.** *$A \subset B \subset E$. On dit que A est* dense *dans B lorsque $B \subset \overline{A}$.*

Proposition 32.29. *$A \subset \mathbb{R}$ est dense dans $\mathbb{R}$* ssi *tout intervalle ouvert de $\mathbb{R}$ contient un élément de A.*

II.3 Topologie induite

Définition 32.30 (Voisinage, ouvert, fermé dans un sous-ensemble)**.** *$A \subset E$. On dit que $X \subset A$ est un* voisinage *de $a \in \overline{A}$ (resp. un* ouvert*, un* fermé*)* dans *A (ou relativement à A) lorsque $X = Y \cap A$, où Y est un voisinage de a (resp. un ouvert, un fermé) dans E.*

Proposition 32.31. *$B \subset A \subset E$. B est ouvert relativement à A* ssi *$A \backslash B$ est fermé relativement à A.*

Proposition 32.32. *$B \subset A \subset E$. B est fermé relativement à A* ssi *toute suite d'éléments de B qui converge dans A a sa limite dans B.*

Définition 32.33 (Connexité)**.** *On dit que $A \subset E$ est* connexe *lorsque A n'est pas une partition en deux ensembles ouverts relativement à A.*

Proposition 32.34. *$I \subset \mathbb{R}$ est connexe dans $\mathbb{R}$* ssi *I est un intervalle.*

III Compacité

Définition 32.35 (Valeur d'adhérence)**.** *$(u_n) \in E^{\mathbb{N}}$. $\ell \in E$ est dite* valeur d'adhérence *de (u_n) lorsqu'il existe une suite extraite de (u_n) de limite ℓ.*

Proposition 32.36. *$(u_n) \in E^{\mathbb{N}}$. $\ell \in E$ est valeur d'adhérence de (u_n)* ssi *pour tout voisinage V de ℓ, l'ensemble $\{n \in \mathbb{N},\, u_n \in V\}$ est infini.*

Définition 32.37 (Compact)**.** *On dit que $K \subset E$ est un* compact *lorsque toute suite de K admet au moins une valeur d'adhérence dans K.*

Proposition 32.38.

(i) *Un compact est fermé et borné.*

(ii) *$K \subset E$ un compact, $X \subset K$. Alors X est fermé* ssi *X est compact.*

(iii) *L'intersection d'un compact et d'un fermé est un compact.*

(iv) *Tout produit fini de compacts est un compact pour la norme produit.*

Notation 32.39. *On suppose E de dimension finie, de base $(e_1, \dots, e_p)$. Pour $x \in E$ de composantes $(x_1, \dots, x_p)$ dans la base $(e_1, \dots, e_p)$, on définit*

$$\|x\|_\infty = \max_{1 \leqslant i \leqslant p} |x_i| .$$

Corollaire 32.40. *On suppose E de dimension finie, muni de $\|\cdot\|_\infty$. Alors toute boule fermée de E est compacte.*

Théorème 32.41. *On suppose E de dimension finie, muni de $\|\cdot\|_\infty$. Alors les compacts de E sont les fermés bornés.*

Théorème 32.42.

(i) *Une suite à valeurs dans un compact ayant une seule valeur d'adhérence converge.*

(ii) *Une suite bornée à valeurs dans un espace vectoriel de dimension finie ayant une seule valeur d'adhérence converge.*

IV Fonctions continues entre deux espaces vectoriels normés

IV.1 Généralités

Notation 32.43. *Dans toute la suite, E, F et G sont des $\mathbb{K}$-espaces vectoriels munis de normes respectives $\|\cdot\|_E$, $\|\cdot\|_F$ et $\|\cdot\|_G$.*

Définition 32.44 (Limite d'une fonction)**.** *$f : A \subset E \to F$. $a \in \overline{A}$.*

(i) *On dit que $\lim_a f = \ell \in F$ lorsque*

$$\forall V \text{ voisinage de } \ell,\ \exists W \text{ voisinage de } a,\ f(W \cap A) \subset V.$$

(ii) *On dit que $\lim_a f = +\infty$ lorsque*

$$\forall M > 0,\ \exists W \text{ voisinage de } a,\ f(W \cap A) \subset F \backslash \mathcal{B}_o(0, M).$$

Définition 32.45 (Continuité)**.** *$f : A \subset E \to F$ est dite* continue *en $a \in A$ lorsque $\lim_a f = f(a)$. On note $\mathcal{C}^0(A, F)$ l'ensemble des fonctions $A \to F$ continues sur A (i.e. en tout point de A).*

Proposition 32.46. *$f : A \subset E \to F$. $a \in \overline{A}$. Alors $\lim_a f = \ell \in F$* ssi

$$\forall (a_n) \in A^{\mathbb{N}},\ a_n \xrightarrow[n\to+\infty]{} a \Longrightarrow f(a_n) \xrightarrow[n\to+\infty]{} \ell.$$

Proposition 32.47. *$f : A \subset E \to F$. On a équivalence entre :*

(i) *f est $\mathcal{C}^0$ sur A.*

(ii) *Pour tout fermé $G \subset F$, $f^{-1}(G)$ est fermé dans A.*

(iii) *Pour tout ouvert $\Omega \subset F$, $f^{-1}(\Omega)$ est ouvert dans A.*

IV.2 Opérations et continuité

Proposition 32.48. *$A \subset E$.*

(i) *$\mathcal{C}^0(A, F)$ est un $\mathbb{K}$-espace vectoriel.*

(ii) *Toute fonction $\mathcal{C}^0$ en $a \in A$ est bornée au voisinage de a.*

(iii) *On suppose que F est une $\mathbb{K}$-algèbre et que $\forall (x, y) \in F^2$, $\|xy\|_F \leqslant \|x\|_F \cdot \|y\|_F$. Alors $\mathcal{C}^0(A, F)$ est une $\mathbb{K}$-algèbre.*

Proposition 32.49. *$f : A \subset E \to F$ et $g : B \subset F \to G$ deux fonctions $\mathcal{C}^0$, avec $f(A) \subset B$. Alors $g \circ f$ est $\mathcal{C}^0$ sur A.*

Corollaire 32.50. *Si $(\lambda_J)_{J \in \mathbb{N}^n}$ est une famille presque nulle d'éléments de $\mathbb{K}$, alors la fonction*

$$f : (x_1, \ldots, x_n) \in \mathbb{K}^n \longmapsto \sum_{(k_1,\ldots,k_n) \in \mathbb{N}^n} \lambda_{(k_1,\ldots,k_n)} \prod_{i=1}^{n} x_i^{k_i},$$

dite polynomiale*, est continue sur $\mathbb{K}^n$.*

Proposition 32.51. *$\det : \mathbb{M}_n(\mathbb{K}) \to \mathbb{K}$ est polynomiale.*

Corollaire 32.52. *$GL_n(\mathbb{K})$ est un ouvert car $GL_n(\mathbb{K}) = \det^{-1}(\mathbb{K}^*)$.*

Remarque 32.53. *$GL_n(\mathbb{K})$ n'est pas un fermé car $\frac{1}{k} I_n \xrightarrow[k\to+\infty]{} 0$.*

V Connexité par arcs

Définition 32.54 (Chemin continu)**.** $(a,b) \in E^2$, $A \subset E$.

(i) *On appelle* chemin continu joignant a à b *toute application* $\gamma \in \mathcal{C}^0([0,1],E)$ *t.q.* $\gamma(0) = a$ *et* $\gamma(1) = b$.

(ii) *On appelle* chemin continu dans A joignant a à b *tout chemin continu* γ *joignant* a *à* b *t.q.* $\gamma([0,1]) \subset A$.

Définition 32.55 (Composantes connexes par arcs)**.** $A \subset E$. *On définit une relation* $\mathcal{R}$ *sur* A *par* $a\mathcal{R}b$ ssi *il existe un chemin continu dans* A *joignant* a *à* b. *Alors* $\mathcal{R}$ *est une relation d'équivalence, et ses classes sont dites* composantes connexes par arcs *de* A.

Définition 32.56 (Ensemble connexe par arcs)**.** $A \subset E$ *est dit* connexe par arcs *lorsque pour tout* $(a,b) \in A^2$, *il existe un chemin continu dans* A *joignant* a *et* b.

Proposition 32.57. *Tout convexe est connexe par arcs.*

Proposition 32.58. *L'image d'un ensemble connexe par arcs par une application* $\mathcal{C}^0$ *est connexe par arcs.*

Proposition 32.59. *Les connexes par arcs de* $\mathbb{R}$ *sont les intervalles.*

Chapitre 33

Théorie de Galois

Cours de Nicolas Tosel

I Polynômes irréductibles

Notation 33.1. *Dans toute la suite, $\mathbb{K}$ est un corps quelconque.*

I.1 Généralités

Proposition 33.2. *Les deux propriétés suivantes sont équivalentes :*

(i) *Les polynômes irréductibles de $\mathbb{K}[X]$ sont les polynômes de degré 1.*

(ii) *Tout polynôme non constant de $\mathbb{K}[X]$ admet une racine dans $\mathbb{K}$.*

Si tel est le cas, on dit que $\mathbb{K}$ est algébriquement clos.

Théorème 33.3 (Théorème de Steinitz)**.** *Si $\mathbb{K}$ est un corps, alors il existe un sur-corps Ω algébriquement clos de $\mathbb{K}$.*

I.2 Corps des rationnels

Exemple 33.4. *Pour $n \in \mathbb{N}^*$, $(X^n - 2)$ est irréductible sur $\mathbb{Q}$.*

Démonstration. Écrire $X^n - 2 = \prod_{\omega \in \mathbb{U}_n} \left(X - \omega 2^{1/n}\right)$. Tout polynôme unitaire Q divisant $(X^n - 2)$ est donc de la forme $Q = \prod_{\omega \in A} \left(X - \omega 2^{1/n}\right)$, où $A \in \mathcal{P}(\mathbb{U}_n)$. En regardant le terme constant de Q, en déduire une contradiction si $1 \leqslant \deg Q \leqslant n-1$. □

Notation 33.5. *Pour $p \in \mathbb{P}$, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On définit alors la* réduction modulo *p : pour $A = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$, on pose $\overline{A} = \sum_{k=0}^n \overline{a_k} X^k \in \mathbb{F}_p[X]$, où $\overline{a_k}$ est la classe d'équivalence de a_k dans $\mathbb{F}_p$.*

Proposition 33.6. $\forall (A,B) \in \mathbb{Z}[X]^2$, $\begin{cases} \overline{A+B} = \overline{A} + \overline{B} \\ \overline{A \times B} = \overline{A} \times \overline{B} \end{cases}$.

Définition 33.7 (Contenu)**.** *Soit $P = \sum_{k=0}^n \lambda_k X^k \in \mathbb{Z}[X] \backslash \{0\}$. On définit le* contenu *de P par :*

$$\mathcal{C}(P) = \bigwedge_{k=0}^{n} \lambda_k.$$

Vocabulaire 33.8 (Polynômes primitifs)**.** $P \in \mathbb{Z}[X]$*. Si* $\mathcal{C}(P) = 1$*,* P *est dit* primitif*.*

Lemme 33.9 (Lemme de Gauss)**.** $\forall (P, Q) \in \mathbb{Z}[X]^2$*,* $\mathcal{C}(PQ) = \mathcal{C}(P)\mathcal{C}(Q)$*.*

Démonstration. Écrire $P = \mathcal{C}(P)\widetilde{P}$, $Q = \mathcal{C}(Q)\widetilde{Q}$, où $\widetilde{P}$ et $\widetilde{Q}$ sont des polynômes primitifs de $\mathbb{Z}[X]$. On a alors $PQ = \mathcal{C}(P)\mathcal{C}(Q)\widetilde{P}\widetilde{Q}$. Supposer alors par l'absurde $\widetilde{P}\widetilde{Q}$ non primitif. Dans ce cas, il existe $p \in \mathbb{P}$ t.q. $p \mid \mathcal{C}\left(\widetilde{P}\widetilde{Q}\right)$. Alors $\overline{\widetilde{P}} \times \overline{\widetilde{Q}} = \overline{\widetilde{P}\widetilde{Q}} = 0_{\mathbb{F}_p[X]}$. Or $\mathbb{F}_p$ est un corps donc $\mathbb{F}_p[X]$ est intègre d'où $\overline{\widetilde{P}} = 0_{\mathbb{F}_p[X]}$ ou $\overline{\widetilde{Q}} = 0_{\mathbb{F}_p[X]}$. C'est une contradiction car $\widetilde{P}$ et $\widetilde{Q}$ sont primitifs. Ainsi $\widetilde{P}\widetilde{Q}$ est primitif et $\mathcal{C}(PQ) = \mathcal{C}(P)\mathcal{C}(Q)$. □

Corollaire 33.10. *Si* $P \in \mathbb{Z}[X]$ *n'a pas de diviseur non constant dans* $\mathbb{Z}[X]$*, alors* P *est irréductible dans* $\mathbb{Q}[X]$*.*

Démonstration. Supposer $P = AB \in \mathbb{Z}[X]$, avec $(A, B) \in (\mathbb{Q}[X] \backslash \mathbb{Q}_0[X])^2$. Écrire $aA \in \mathbb{Z}[X]$, $bB \in \mathbb{Z}[X]$ avec $(a, b) \in (\mathbb{Z}^*)^2$. Noter que $ab\mathcal{C}(P) = \mathcal{C}(abP) = \mathcal{C}(aA)\mathcal{C}(bB)$, et qu'il existe $(A_1, B_1) \in \mathbb{Z}[X]^2$ t.q. $aA = \mathcal{C}(aA)A_1$ et $bB = \mathcal{C}(bB)B_1$. Écrire enfin P sous forme d'un produit de polynômes non constants de $\mathbb{Z}[X]$ et en déduire le résultat par contraposée. □

Théorème 33.11 (Théorème d'Eisenstein)**.** $Q = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$*,* $p \in \mathbb{P}$*.*

$$\left.\begin{array}{r} \forall k \in [\![0, n[\![,\ p \mid a_k \\ p \nmid a_n \\ p^2 \nmid a_0 \end{array}\right\} \Longrightarrow Q \text{ est irréductible sur } \mathbb{Q}.$$

Démonstration. Supposer par l'absurde $Q = AB$, avec $(A, B) \in (\mathbb{Z}[X] \backslash \mathbb{Z}_0[X])^2$. Effectuer la réduction de Q modulo p : $\overline{A} \times \overline{B} = \overline{Q} = \overline{a_n} X^n$. En déduire que $\overline{A}$ et $\overline{B}$ sont des monômes dans $\mathbb{F}_p[X]$. Donc p divise les coefficients constants respectifs de A et B ; donc p^2 divise a_0. Contradiction. □

I.3 Cyclotomie

Définition 33.12 (Polynômes cyclotomiques)**.** *Pour* $n \in \mathbb{N}^*$*, on définit le* n*-ième* polynôme cyclotomique *par :*

$$\Phi_n = \prod_{\substack{k \in [\![1,n]\!] \\ k \wedge n = 1}} \left(X - e^{\frac{2ik\pi}{n}}\right).$$

Lemme 33.13. $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d|n} \Phi_d$.

Proposition 33.14. $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

Démonstration. Par récurrence forte sur n, en utilisant la division euclidienne de $(X^n - 1)$ par $\prod_{\substack{d|n \\ d<n}} \Phi_d$ dans $\mathbb{Z}[X]$. □

I.4 Séparabilité

Définition 33.15 (Caractéristique d'un anneau)**.** $\mathbb{A}$ *un anneau. Si* $\exists n \in \mathbb{N}^*$, $n \cdot 1_{\mathbb{A}} = \underbrace{1_{\mathbb{A}} + 1_{\mathbb{A}} + \cdots + 1_{\mathbb{A}}}_{n \text{ fois}} = 0_{\mathbb{A}}$*, alors on appelle* caractéristique *de* $\mathbb{A}$ *l'entier* $\min\{n \in \mathbb{N}^*,\ n \cdot 1_{\mathbb{A}} = 0_{\mathbb{A}}\}$*.*
Sinon, on dit que $\mathbb{A}$ *est de caractéristique* 0*.*

Définition 33.16 (Séparabilité)**.** $P \in \mathbb{K}[X]$*. On dit que* P *est* séparable *si les racines de* P *dans un sur-corps de* $\mathbb{K}$ *scindant* P *sont simples. Autrement dit,* P *est séparable* ssi $P \wedge P' = 1$*.*

Proposition 33.17. $\mathbb{K}$ *un corps de caractéristique* 0*. Si* $P \in \mathbb{K}[X]$ *est irréductible, alors* P *est séparable.*

Démonstration. On note $n = \deg P$. Comme $\mathbb{K}$ est de caractéristique 0, $\deg P' = n - 1$. En particulier, $P' \neq 0$ (car $n \geqslant 1$ car P est non constant). P est irréductible et $0 \leqslant \deg P' < \deg P$ donc $P \wedge P' = 1$. □

Proposition 33.18. $\mathbb{K}$ *un corps de caractéristique* p*.* $P \in \mathbb{K}[X]$ *irréductible. Alors* P *est séparable* ssi $P \notin \mathbb{K}[X^p]$*.*

II Extensions de corps

II.1 Extensions et degrés

Définition 33.19 (Extension de corps)**.** *Si* $\mathbb{K}$ *est un sous-corps d'un corps* $\mathbb{L}$*, on dit que* $\mathbb{L}/\mathbb{K}$ *est une* extension*. On dit de plus que* $\mathbb{L}/\mathbb{K}$ *est finie si le* $\mathbb{K}$*-espace vectoriel* $\mathbb{L}$ *est de dimension finie. Dans ce cas, le* degré *de* $\mathbb{L}/\mathbb{K}$*, noté* $[\mathbb{L} : \mathbb{K}]$*, est par définition la dimension de cet espace vectoriel.*

Théorème 33.20 (Théorème de la base télescopique)**.** $\mathbb{L}/\mathbb{K}$ *et* $\mathbb{M}/\mathbb{L}$ *deux extensions. Soit* $(e_i)_{i\in I}$ *une base de* $\mathbb{L}/\mathbb{K}$*,* $(f_j)_{j\in J}$ *une base de* $\mathbb{M}/\mathbb{L}$*. Alors* $(e_i f_j)_{(i,j)\in I\times J}$ *est une base de* $\mathbb{M}/\mathbb{K}$*.*

Corollaire 33.21. $\mathbb{L}/\mathbb{K}$ *et* $\mathbb{M}/\mathbb{L}$ *deux extensions. Si* $\mathbb{L}/\mathbb{K}$ *et* $\mathbb{M}/\mathbb{L}$ *sont finies, alors* $\mathbb{M}/\mathbb{K}$ *aussi, et dans ce cas :*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}].$$

II.2 Adjonction, éléments algébriques et transcendants

Proposition 33.22. $\mathbb{L}/\mathbb{K}$ *une extension.* $(x_1, \ldots, x_n) \in \mathbb{L}^n$*.*

(i) *Le plus petit sous-anneau de* $\mathbb{L}$ *contenant* $\mathbb{K}$ *et tous les* x_i *est :*

$$\mathbb{K}[x_1, \ldots, x_n] = \{P(x_1, \ldots, x_n),\ P \in \mathbb{K}[X_1, \ldots, X_n]\}.$$

(ii) *Le plus petit sous-corps de* $\mathbb{L}$ *contenant* $\mathbb{K}$ *et tous les* x_i *est :*

$$\mathbb{K}(x_1, \ldots, x_n) = \{P(x_1, \ldots, x_n),\ P \in \mathbb{K}(X_1, \ldots, X_n)\}.$$

Définition 33.23 (Éléments algébriques et transcendants)**.** $x \in \mathbb{L}$*. On dit que* x *est* algébrique *sur* $\mathbb{K} \subset \mathbb{L}$ *lorsque* $\exists P \in \mathbb{K}[X]\backslash\{0\}$, $P(x) = 0$*. Si* x *n'est pas algébrique, on dit que* x *est* transcendant*.*

Notation 33.24. $x \in \mathbb{L}$ *algébrique sur* $\mathbb{K}$*. On introduit :*

(i) *L'*idéal annulateur *de* x *:* $I_{\mathbb{K},x} = \{P \in \mathbb{K}[X],\ P(x) = 0\}$*.*

(ii) *Le* polynôme minimal *de* x *:* $\Pi_{\mathbb{K},x}$ *unitaire t.q.* $I_{\mathbb{K},x} = \Pi_{\mathbb{K},x}\mathbb{K}[X]$*.*

De plus, le degré de $\Pi_{\mathbb{K},x}$ *est dit* degré d'algébricité *de* x *sur* $\mathbb{K}$*.*

Proposition 33.25. $x \in \mathbb{L}$ *algébrique sur* $\mathbb{K}$*.*

(i) $\Pi_{\mathbb{K},x}$ *est irréductible sur* $\mathbb{K}$.

(ii) *Si* $P \in \mathbb{K}[X]$ *est irréductible unitaire et* $P(x) = 0$, *alors* $\Pi_{\mathbb{K},x} = P$.

Théorème 33.26. $x \in \mathbb{L}$ *algébrique de degré* d *sur* $\mathbb{K}$.

(i) $\left(x^k\right)_{k\in[\![0,d[\![}$ *est une* $\mathbb{K}$*-base de* $\mathbb{K}[x]$.

(ii) $\mathbb{K}[x]$ *est un sous-corps de* $\mathbb{L}$, *donc* $\mathbb{K}[x] = \mathbb{K}(x)$.

Ainsi, $\mathbb{K}(x)/\mathbb{K}$ *est une extension et* $[\mathbb{K}(x) : \mathbb{K}] = d$.

Démonstration. (i) Si $\left(x^k\right)_{k\in[\![0,d[\![}$ n'était pas libre, il existerait $P \in \mathbb{K}_{d-1}[X]$ t.q. $P(x) = 0$, ce qui contredit la définition du degré d'algébricité. Pour montrer que $\left(x^k\right)_{k\in[\![0,d[\![}$ est génératrice, utiliser la division euclidienne par $\Pi_{\mathbb{K},x}$. (ii) Soit $y = P(x) \in \mathbb{K}[x]\backslash\{0\}$. Par ce qui précède, on peut supposer $P \in \mathbb{K}_{d-1}[X]$. Or $\Pi_{\mathbb{K},x}$ est irréductible et $\deg \Pi_{\mathbb{K},x} = d$, donc $P \wedge \Pi_{\mathbb{K},x} = 1$. Utiliser alors l'égalité de Bézout pour écrire $PU + \Pi_{\mathbb{K},x}V = 1$, où $(U, V) \in \mathbb{K}[X]^2$. En déduire que $P(x)U(x) = 1$, d'où l'inversibilité de $y = P(x)$. □

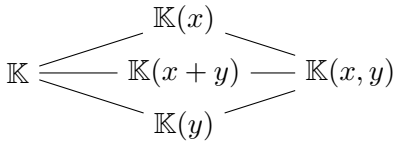
II.3 Sommes et produits d'algébriques

Proposition 33.27. $(x, y) \in \mathbb{L}^2$ *algébriques sur* $\mathbb{K}$ *de degrés respectifs* d_x *et* d_y. *Alors :*

(i) $(x + y)$ *est algébrique sur* $\mathbb{K}$ *de degré au plus* $d_x d_y$,

(ii) $(x \times y)$ *est algébrique sur* $\mathbb{K}$ *de degré au plus* $d_x d_y$.

Démonstration. L'extension $\mathbb{K}(x, y)/\mathbb{K}(x)$ est finie de degré au plus d_y et l'extension $\mathbb{K}(x)/\mathbb{K}$ est finie de degré d_x donc l'extension $\mathbb{K}(x, y)/\mathbb{K}$ est finie de degré au plus $d_x d_y$. Or $\mathbb{K}(x + y) \subset \mathbb{K}(x, y)$ et $\mathbb{K}(x \times y) \subset \mathbb{K}(x, y)$, d'où le résultat.



□

II.4 Extensions finies et algébriques

Proposition 33.28. *Une extension* $\mathbb{L}/\mathbb{K}$ *est finie* ssi *il existe* $(x_1, \ldots, x_n) \in \mathbb{L}^n$ *algébriques sur* $\mathbb{K}$ *tels que* $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_n)$.

Démonstration. ($\Rightarrow$) Soit $(x_1, \ldots, x_n)$ une $\mathbb{K}$-base de $\mathbb{L}$. Montrer que $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_n)$ et que $x_1, \ldots, x_n$ sont algébriques sur $\mathbb{K}$. ($\Leftarrow$) Par récurrence sur n. □

Définition 33.29 (Extension algébrique)**.** *On dit qu'une extension* $\mathbb{L}/\mathbb{K}$ *est* algébrique *lorsque tout élément de* $\mathbb{L}$ *est algébrique sur* $\mathbb{K}$.

Proposition 33.30. *Si une extension* $\mathbb{L}/\mathbb{K}$ *est finie, alors elle est algébrique.*

Notation 33.31. *On note* $\overline{\mathbb{Q}}$ *l'ensemble des* $x \in \mathbb{C}$ *algébriques sur* $\mathbb{Q}$.

Proposition 33.32. $\overline{\mathbb{Q}}$ *est un sous-corps de* $\mathbb{C}$ *et* $\overline{\mathbb{Q}}/\mathbb{Q}$ *est une extension algébrique non finie.*

Théorème 33.33. $\overline{\mathbb{Q}}$ *est algébriquement clos.*

Démonstration. Soit $P = \sum_{k=0}^{n} a_k X^k \in \overline{\mathbb{Q}}[X] \backslash \overline{\mathbb{Q}}_0[X]$. Soit $z \in \mathbb{C}$ une racine de P (qui existe par le théorème de d'Alembert-Gauss). L'extension $\mathbb{Q}(a_0, \ldots, a_n)/\mathbb{Q}$ est finie car $a_0, \ldots, a_n$ sont algébriques sur $\mathbb{Q}$ et l'extension $\mathbb{Q}(a_0, \ldots, a_n, z)/\mathbb{Q}(a_0, \ldots, a_n)$ est finie car z est algébrique sur $\mathbb{Q}(a_0, \ldots, a_n)$ (puisque $P(z) = 0$). Donc l'extension $\mathbb{Q}(a_0, \ldots, a_n, z)/\mathbb{Q}$ est finie ; or, $\mathbb{Q} \subset \mathbb{Q}(z) \subset \mathbb{Q}(a_0, \ldots, a_n, z)$ donc $\mathbb{Q}(z)/\mathbb{Q}$ est finie et $z \in \overline{\mathbb{Q}}$. □

II.5 Théorème de l'élément primitif

Définition 33.34 (Extension monogène)**.** *On dit qu'une extension $\mathbb{L}/\mathbb{K}$ est* monogène *lorsque $\exists x \in \mathbb{L}$, $\mathbb{L} = \mathbb{K}(x)$.*

Théorème 33.35 (Théorème de l'élément primitif)**.** *$\mathbb{K}$ un corps de caractéristique 0. Si l'extension $\mathbb{L}/\mathbb{K}$ est finie, alors elle est monogène : il existe $x \in \mathbb{L}$ t.q. $\mathbb{L} = \mathbb{K}(x)$. On dit alors que x est un élément primitif de $\mathbb{L}/\mathbb{K}$.*

Démonstration. Il suffit de montrer que, si $\mathbb{L} = \mathbb{K}(x, y)$, alors $\exists z \in \mathbb{L}$, $\mathbb{L} = \mathbb{K}(z)$ (généraliser ensuite par récurrence sur le nombre de générateurs). Soit Ω un sur-corps de $\mathbb{K}$ algébriquement clos. Alors $\Pi_{\mathbb{K},x}$ et $\Pi_{\mathbb{K},y}$ sont scindés sur Ω, et à racines simples car $\mathbb{K}$ est de caractéristique 0 (et $\Pi_{\mathbb{K},x}$ et $\Pi_{\mathbb{K},y}$ sont irréductibles donc séparables). Écrire alors $\Pi_{\mathbb{K},x} = \prod_{i=1}^{m}(X - x_i)$ et $\Pi_{\mathbb{K},y} = \prod_{i=1}^{n}(X - y_i)$, avec $x_1 = x$, $y_1 = y$. Soit $t \in \mathbb{K}$ t.q. $\forall (i,j) \neq (1,1)$, $x + ty \neq x_i + ty_j$. Soit $z = x + ty$. On va montrer que $\mathbb{K}(z) = \mathbb{K}(x, y)$. L'inclusion $\subset$ est claire. Pour montrer $\supset$, il suffit de prouver que $\mathbb{K}(y) \subset \mathbb{K}(z)$, car on aura alors $x = z - ty \in \mathbb{K}(z)$. Soit $P_1 = \Pi_{\mathbb{K},y} \in \mathbb{K}(z)[X]$, $P_2 = \Pi_{\mathbb{K},x}(z - tX) \in \mathbb{K}(z)[X]$. Montrer que $P_1(y) = P_2(y) = 0$, d'où $(X - y) \mid P_1$ et $(X - y) \mid P_2$. Justifier que P_1 et P_2 n'admettent pas d'autre diviseur commun et en déduire que $P_1 \wedge P_2 = X - y$. Ainsi, $(X - y) \in \mathbb{K}(z)[X]$ donc $y \in \mathbb{K}(z)$, d'où $\mathbb{K}(y) \subset \mathbb{K}(z)$. □

Théorème 33.36. *$\mathbb{L}/\mathbb{K}$ une extension finie. Si $\mathbb{L}/\mathbb{K}$ est monogène alors il n'existe qu'un nombre fini de sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$.*

Démonstration. Soit $\mathbb{M}$ un sous-corps de $\mathbb{L} = \mathbb{K}(x)$ contenant $\mathbb{K}$. On note $X^d + \sum_{k=0}^{d-1} a_k X^k = \Pi_{\mathbb{M},x}$. Comme $\Pi_{\mathbb{M},x} \mid \Pi_{\mathbb{K},x}$, on n'a qu'un nombre fini de choix pour $\Pi_{\mathbb{M},x}$. Or $\mathbb{M} = \mathbb{K}(a_0, \ldots, a_{d-1})$. En effet, l'inclusion $\supset$ est claire. Et réciproquement $[\mathbb{L} : \mathbb{M}] = d$; or x est de degré inférieur ou égal à d sur $\mathbb{K}(a_0, \ldots, a_{d-1})$, d'où $\mathbb{M} = \mathbb{K}(a_0, \ldots, a_{d-1})$. Donc on n'a qu'un nombre fini de choix pour $\mathbb{M}$. □

Corollaire 33.37. *Si $\mathbb{K}$ est un corps de caractéristique 0 et $\mathbb{L}/\mathbb{K}$ est une extension finie, alors il n'existe qu'un nombre fini de sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$.*

II.6 Irréductibilité des polynômes cyclotomiques

Définition 33.38 (Entier algébrique)**.** *On dit que $z \in \mathbb{C}$ est un* entier algébrique *lorsqu'il existe $P \in \mathbb{Z}[X]$ unitaire t.q. $P(z) = 0$.*

Lemme 33.39. *$z \in \mathbb{C}$ est un entier algébrique* ssi *$z \in \overline{\mathbb{Q}}$ et $\Pi_{\mathbb{Q},z} \in \mathbb{Z}[X]$.*

Lemme 33.40. *Si ω est une racine primitive n-ième de l'unité et si $p \in \mathbb{P}$ ne divise pas n alors ω^p est racine de $\Pi_{\mathbb{Q},\omega}$.*

Démonstration. ω et ω^p étant des entiers algébriques, on a $\Pi_{\mathbb{Q},\omega} \in \mathbb{Z}[X]$ et $\Pi_{\mathbb{Q},\omega^p} \in \mathbb{Z}[X]$. De plus, $\Pi_{\mathbb{Q},\omega^p}(X^p)$ annule ω donc $\Pi_{\mathbb{Q},\omega} \mid \Pi_{\mathbb{Q},\omega^p}(X^p)$. Le quotient est dans $\mathbb{Z}[X]$ car $\Pi_{\mathbb{Q},\omega}$ est unitaire : $\exists A \in \mathbb{Z}[X]$, $\Pi_{\mathbb{Q},\omega^p}(X^p) = A\Pi_{\mathbb{Q},\omega}$. Or $\overline{\Pi_{\mathbb{Q},\omega^p}}(X^p) = \overline{\Pi_{\mathbb{Q},\omega^p}}^p$, donc $\overline{\Pi_{\mathbb{Q},\omega^p}}^p = \overline{A} \cdot \overline{\Pi_{\mathbb{Q},\omega}}$. Mais, si $\Pi_{\mathbb{Q},\omega} \neq \Pi_{\mathbb{Q},\omega^p}$, alors $(\Pi_{\mathbb{Q},\omega}\Pi_{\mathbb{Q},\omega^p}) \mid (X^n - 1)$ dans $\mathbb{Z}[X]$. Soit alors $x \in \overline{\mathbb{F}}_p$

racine de $\overline{\Pi_{\mathbb{Q},\omega}}$ ($\overline{\mathbb{F}}_p$ est un sur-corps de $\mathbb{F}_p$ algébriquement clos), alors x est racine de $\overline{\Pi_{\mathbb{Q},\omega^p}}$ donc x est racine multiple de $\overline{X^n-1}$, ce qui est absurde car $\left(\overline{X^n-1}\right)' = \overline{nX^{n-1}} \neq 0$ (car $p \nmid n$), donc $\overline{X^n-1} \wedge \left(\overline{X^n-1}\right)' = 1$. Donc $\Pi_{\mathbb{Q},\omega} = \Pi_{\mathbb{Q},\omega^p}$. □

Théorème 33.41 (Théorème de Gauss-Kronecker)**.** *$\forall n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Q}$.*

III Extensions et morphismes

III.1 Applications préservant les relations algébriques

Lemme 33.42. *$\mathbb{A}$ et $\mathbb{A}'$ deux $\mathbb{K}$-algèbres. Alors $\varphi : \mathbb{A} \to \mathbb{A}'$ est un morphisme de $\mathbb{K}$-algèbres* ssi *$\forall n \in \mathbb{N}^*$, $\forall P \in \mathbb{K}[X_1, \ldots, X_n]$, $\forall (x_1, \ldots, x_n) \in \mathbb{A}^n$, $\varphi(P(x_1, \ldots, x_n)) = P(\varphi(x_1), \ldots, \varphi(x_n))$.*

Notation 33.43. *Dans toute la suite, $\mathbb{K}$ est un corps et Ω est une* clôture algébrique *de $\mathbb{K}$ (i.e. un sur-corps de $\mathbb{K}$ algébriquement clos t.q. l'extension $\Omega/\mathbb{K}$ est algébrique).*

Notation 33.44. *$\mathbb{L}$ et $\mathbb{M}$ deux sous-corps de Ω.*

(i) *On note* $\mathrm{Hom}(\mathbb{L}, \mathbb{M})$ *l'ensemble des morphismes de corps $\mathbb{L} \to \mathbb{M}$.*

(ii) *On note* $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{M})$ *l'ensemble des morphismes de $\mathbb{K}$-algèbres $\mathbb{L} \to \mathbb{M}$.*

Notation 33.45. *Pour $P = \sum_{k\in\mathbb{N}} \lambda_k X^k \in \mathbb{L}[X]$, $\sigma \in \mathrm{Hom}(\mathbb{L}, \mathbb{M})$, on note $\sigma \cdot P = \sum_{k\in\mathbb{N}} \sigma(\lambda_k) X^k \in \mathbb{M}[X]$.*

III.2 Conjugaison

Définition 33.46 (Conjugaison)**.** *$(x, y) \in \Omega^2$. On dit que x et y sont* $\mathbb{K}$-conjugués *lorsque $\Pi_{\mathbb{K},x} = \Pi_{\mathbb{K},y}$.*

Proposition 33.47. *$x \in \Omega$. Si $\Pi_{\mathbb{K},x}$ est séparable sur $\mathbb{K}$ (ce qui est vrai dès que $\mathbb{K}$ est de caractéristique 0), alors x a exactement $(\deg \Pi_{\mathbb{K},x})$ $\mathbb{K}$-conjugués.*

Proposition 33.48. *$(x, y) \in \Omega^2$. Alors x et y sont $\mathbb{K}$-conjugués* ssi *$\exists \sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(x), \Omega), \sigma(x) = y$. Dans ce cas, σ est unique.*

Démonstration. ($\Leftarrow$) $\Pi_{\mathbb{K},x}(y) = \Pi_{\mathbb{K},x}(\sigma(x)) = 0$. ($\Rightarrow$) *Analyse.* Si σ existe, alors $\forall P \in \mathbb{K}[X]$, $\sigma(P(x)) = P(\sigma(x)) = P(y)$. En déduire qu'il existe au plus un σ qui convient. *Synthèse.* Montrer que l'application $\sigma : \left|\begin{array}{l}\mathbb{K}[x] \longrightarrow \Omega \\ P(x) \longmapsto P(y)\end{array}\right.$ est bien définie et qu'elle convient. Comme $\mathbb{K}[x] = \mathbb{K}(x)$, en déduire le résultat. □

III.3 Prolongement des morphismes

Théorème 33.49. *$\mathbb{L}/\mathbb{K}$ et $\mathbb{L}'/\mathbb{K}'$ deux extensions. $\sigma : \mathbb{K} \to \mathbb{K}'$ un isomorphisme de corps. $x \in \mathbb{L}$ algébrique sur $\mathbb{K}$, $x' \in \mathbb{L}'$. Alors les deux propriétés suivantes sont équivalentes :*

(i) *Il existe $\sigma' \in \mathrm{Hom}(\mathbb{K}(x), \mathbb{L}')$ prolongeant σ et envoyant x sur x'.*

(ii) *x' est algébrique sur $\mathbb{K}'$ et $\Pi_{\mathbb{K}',x'} = \sigma \cdot \Pi_{\mathbb{K},x}$.*

Dans ce cas, σ est unique.

Démonstration. ($\Rightarrow$) Montrer que $\forall P \in \mathbb{K}[X]$, $\sigma'(P(x)) = \sigma \cdot P(x')$. En déduire le résultat, en notant que $\sigma \cdot \Pi_{\mathbb{K},x}$ est irréductible unitaire car σ est un isomorphisme. ($\Leftarrow$) L'application $\Phi : \left| \begin{array}{l} \mathbb{K}[X] \longrightarrow \mathbb{L}' \\ P \longmapsto \sigma \cdot P(x') \end{array} \right.$ est un morphisme d'anneaux et $\operatorname{Ker}\Phi = \Pi_{\mathbb{K},x}\mathbb{K}[X]$. Ceci permet, par passage au quotient, de définir un morphisme d'anneaux $\sigma' : \left| \begin{array}{l} \mathbb{K}[x] \longrightarrow \mathbb{L}' \\ P(x) \longmapsto \sigma \cdot P(x') \end{array} \right.$. □

Corollaire 33.50.

(i) *Si $x \in \Omega$ (donc x algébrique), alors tout élément de* $\mathrm{Hom}(\mathbb{K}, \Omega)$ *admet autant de prolongements en un élément de* $\mathrm{Hom}(\mathbb{K}(x), \Omega)$ *que le nombre de $\mathbb{K}$-conjugués de x.*

(ii) *Si $\mathbb{L}/\mathbb{K}$ est une extension finie, alors tout élément de* $\mathrm{Hom}(\mathbb{K}, \Omega)$ *admet au moins un prolongement en un élément de* $\mathrm{Hom}(\mathbb{L}, \Omega)$.

(iii) *Si $\mathbb{M}/\mathbb{L}$ et $\mathbb{L}/\mathbb{K}$ sont des extensions finies, alors tout élément de* $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$ *peut se prolonger en un élément de* $\mathrm{Hom}_{\mathbb{K}}(\mathbb{M}, \Omega)$.

III.4 Conséquences

Théorème 33.51. *$\mathbb{L}/\mathbb{K}$ une extension finie, où $\mathbb{K}$ est de caractéristique 0. Alors :*

$$|(\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega))| = [\mathbb{L} : \mathbb{K}]\,.$$

Démonstration. Utiliser le théorème de l'élément primitif (théorème 33.35) pour écrire $\mathbb{L} = \mathbb{K}(x)$. Utiliser ensuite le fait que $|(\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega))|$ est le nombre de $\mathbb{K}$-conjugués de x. □

Théorème 33.52 (Caractérisation du corps de base)**.** *$\mathbb{L}/\mathbb{K}$ une extension finie, où $\mathbb{K}$ est de caractéristique 0. Alors*

$$\mathbb{K} = \{x \in \mathbb{L},\ \forall \sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega),\ \sigma(x) = x\}\,.$$

III.5 Indépendance des morphismes

Théorème 33.53. *$(\mathbb{M}, \cdot)$ un monoïde (ensemble muni d'une LCI associative et d'un élément neutre), $(\mathbb{K}, +, \times)$ un corps. $(\sigma_1, \ldots, \sigma_p)$ des morphismes de $(\mathbb{M}, \cdot)$ dans $(\mathbb{K}^*, \times)$ deux-à-deux distincts. Alors $(\sigma_1, \ldots, \sigma_p)$ sont $\mathbb{K}$-linéairement indépendants.*

Démonstration. Par récurrence sur p. □

IV Théorie de Galois des extensions finies

IV.1 Définition du groupe de Galois

Définition 33.54 (Groupe de Galois)**.** *Si $\mathbb{L}/\mathbb{K}$ est une extension finie, on définit le* groupe de Galois *de $\mathbb{L}/\mathbb{K}$ par*

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{L}) \subset \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega).$$

Proposition 33.55. *$\mathbb{L}/\mathbb{K}$ une extension finie. Alors $(\mathrm{Gal}(\mathbb{L}/\mathbb{K}), \circ)$ est un groupe.*

Vocabulaire 33.56. *$\mathbb{L}/\mathbb{K}$ une extension finie.*

(i) *On dit que* $\mathbb{L}/\mathbb{K}$ *est une* extension normale *lorsque* $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\mathbb{L}) = \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)$*, i.e. lorsque* $\mathbb{L}$ *est stable par* $\mathbb{K}$*-conjugaison.*

(ii) *On dit que* $\mathbb{L}/\mathbb{K}$ *est une* extension séparable *si, pour tout* $x \in \mathbb{L}$*,* $\Pi_{\mathbb{K},x}$ *est séparable.*

(iii) *On dit que* $\mathbb{L}/\mathbb{K}$ *est une* extension galoisienne *lorsque* $\mathbb{L}/\mathbb{K}$ *est une extension normale séparable.*

Remarque 33.57. $\mathbb{L}/\mathbb{K}$ *une extension finie. Si* $\mathbb{K}$ *est de caractéristique* 0*, alors* $\mathbb{L}/\mathbb{K}$ *est galoisienne* ssi $\mathbb{L}/\mathbb{K}$ *est normale (car* $\mathbb{L}/\mathbb{K}$ *est toujours séparable).*

IV.2 Propriétés des extensions normales

Définition 33.58 (Corps de décomposition)**.** $P = \prod_{i=1}^{n}(X - x_i) \in \mathbb{K}[X]$*, avec* $(x_1,\dots,x_n) \in \Omega^n$*. Le corps de décomposition de* P *sur* $\mathbb{K}$ *est par définition*

$$D_{\mathbb{K}}(P) = \mathbb{K}(x_1,\dots,x_n).$$

Théorème 33.59. $\mathbb{L}/\mathbb{K}$ *une extension finie. Alors* $\mathbb{L}/\mathbb{K}$ *est normale* ssi $\exists P \in \mathbb{K}[X]$, $\mathbb{L} = D_{\mathbb{K}}(P)$*.*

Démonstration. ($\Rightarrow$) $\mathbb{L} = \mathbb{K}(x_1,\dots,x_p) = D_{\mathbb{K}}\left(\Pi_{\mathbb{K},x_1}\cdots\Pi_{\mathbb{K},x_p}\right)$ car $\mathbb{L}$ contient les $\mathbb{K}$-conjugués des x_i. ($\Leftarrow$) $\mathbb{L} = D_{\mathbb{K}}(P)$, avec $P = \prod_{i=1}^{n}(X - x_i)$, donc $\mathbb{L} = \mathbb{K}(x_1,\dots,x_n)$. Soit $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)$. Pour tout $i \in [\![1,n]\!]$, $\sigma(x_i)$ annule P donc est l'un des x_j donc est dans $\mathbb{L}$. Donc $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\mathbb{L})$. □

Définition 33.60 (Clôture normale)**.** *La* clôture normale $\mathrm{Clnorm}_{\mathbb{K}}(\mathbb{L})$ *d'une extension finie* $\mathbb{L}/\mathbb{K}$ *est le plus petit sous-corps de* Ω *contenant* $\mathbb{L}$ *et normal sur* $\mathbb{K}$*.*

IV.3 Propriétés simples du groupe de Galois

Notation 33.61. $\mathbb{L}/\mathbb{K}$ *une extension finie. On note :*

(i) $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$ *l'ensemble des sous-corps de* $\mathbb{L}$ *contenant* $\mathbb{K}$*,*

(ii) $\mathcal{G}_{\mathbb{L}/\mathbb{K}}$ *l'ensemble des sous-groupes de* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$*.*

Proposition 33.62. $\mathbb{L}/\mathbb{K}$ *une extension normale,* $\mathbb{K}' \in \mathcal{K}_{\mathbb{L}/\mathbb{K}}$*. Alors l'extension* $\mathbb{L}/\mathbb{K}'$ *est normale.*

Proposition 33.63. $\mathbb{L}/\mathbb{K}$ *une extension finie,* $\mathbb{K}' \in \mathcal{K}_{\mathbb{L}/\mathbb{K}}$*. Alors* $\mathrm{Gal}(\mathbb{L}/\mathbb{K}')$ *est un sous-groupe de* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$*.*

Théorème 33.64 (Théorème de l'irrationalité naturelle)**.** $\mathbb{L}/\mathbb{K}$ *une extension normale.* $(x_1,\dots,x_p) \in \Omega^p$*. Alors* $\mathbb{L}(x_1,\dots,x_p)/\mathbb{K}(x_1,\dots,x_p)$ *est normale et* $\mathrm{Gal}(\mathbb{L}(x_1,\dots,x_p)/\mathbb{K}(x_1,\dots,x_p))$ *est isomorphe à un sous-groupe de* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$*.*

Démonstration. Noter qu'il existe $P \in \mathbb{K}[X]$ tel que $\mathbb{L} = D_{\mathbb{K}}(P)$ donc $\mathbb{L}(x_1,\dots,x_p) = D_{\mathbb{K}(x_1,\dots,x_p)}(P)$. Exhiber de plus un morphisme injectif de $\mathrm{Gal}(\mathbb{L}(x_1,\dots,x_p)/\mathbb{K}(x_1,\dots,x_p))$ dans $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. □

Notation 33.65. $\mathbb{F}$ *un corps,* G *un groupe d'automorphismes de* $\mathbb{F}$*. On note*

$$\mathbb{F}^G = \{x \in \mathbb{F},\ \forall g \in G,\ g(x) = x\}.$$

Proposition 33.66. *Si l'extension* $\mathbb{L}/\mathbb{K}$ *est normale, et si* $\mathbb{K}$ *est de caractéristique* 0*, alors*

$$\mathbb{K} = \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})}.$$

IV.4 Premier volet de la correspondance de Galois

Lemme 33.67 (Lemme d'Artin)**.** $\mathbb{F}$ *un corps de caractéristique* 0*,* G *un groupe d'automorphismes de* $\mathbb{F}$*. Alors l'extension* $\mathbb{F}/\mathbb{F}^G$ *est normale finie et*

$$\mathrm{Gal}\left(\mathbb{F}/\mathbb{F}^G\right) = G.$$

Démonstration. Noter d'abord que $G \subset \mathrm{Gal}\left(\mathbb{F}/\mathbb{F}^G\right)$. On va montrer que $\left[\mathbb{F} : \mathbb{F}^G\right] \leqslant |G|$, d'où le résultat car $\left|\mathrm{Gal}\left(\mathbb{F}/\mathbb{F}^G\right)\right| \leqslant \left[\mathbb{F} : \mathbb{F}^G\right]$, avec égalité ssi $\mathbb{F}/\mathbb{F}^G$ est normale. Comme $\mathbb{F}/\mathbb{F}^G$ est monogène (caractéristique 0), il suffit de prouver que tout $x \in \mathbb{F}$ est de degré inférieur ou égal à $|G|$ sur $\mathbb{F}^G$. Or, pour $x \in \mathbb{F}$, $\prod_{\sigma\in G}(X - \sigma(x))$ est dans $\mathbb{F}^G[X]$, de degré majoré par $|G|$, et annule x. □

Théorème 33.68. $\mathbb{L}/\mathbb{K}$ *une extension normale, avec* $\mathbb{K}$ *de caractéristique* 0*. On définit*

$$\varphi : \left|\begin{array}{l}\mathcal{K}_{\mathbb{L}/\mathbb{K}} \longrightarrow \mathcal{G}_{\mathbb{L}/\mathbb{K}} \\ \mathbb{K}' \longmapsto \mathrm{Gal}(\mathbb{L}/\mathbb{K}')\end{array}\right. \quad \text{et} \quad \psi : \left|\begin{array}{l}\mathcal{G}_{\mathbb{L}/\mathbb{K}} \longrightarrow \mathcal{K}_{\mathbb{L}/\mathbb{K}} \\ G \longmapsto \mathbb{L}^G\end{array}\right. .$$

Alors φ *et* ψ *sont des bijections réciproques.*

V Actions de groupes

V.1 Généralités

Définition 33.69 (Action de groupe)**.** G *un groupe,* X *un ensemble. On appelle* action de G sur X *toute application* $\left|\begin{array}{l}G \times X \longrightarrow X \\ (g,x) \longmapsto g \cdot x\end{array}\right.$ *vérifiant :*

(i) $\forall x \in X,\ e \cdot x = x,$

(ii) $\forall (g_1, g_2) \in G^2,\ \forall x \in X,\ g_2 \cdot (g_1 \cdot x) = (g_2 g_1) \cdot x.$

Proposition 33.70. G *un groupe,* X *un ensemble. Une application* $\left|\begin{array}{l}G \times X \longrightarrow X \\ (g,x) \longmapsto g \cdot x\end{array}\right.$ *est une action de groupe* ssi $\sigma : \left|\begin{array}{l}G \longrightarrow \mathfrak{S}_X \\ g \longmapsto \sigma_g\end{array}\right.$ *est un morphisme, où* $\sigma_g : \left|\begin{array}{l}X \longrightarrow X \\ x \longmapsto g \cdot x\end{array}\right.$*, pour* $g \in G$*. Si* σ *est injectif, on dit que l'action de* G *sur* X *est* fidèle.

Exemple 33.71.

(i) $\mathfrak{S}_n$ *agit sur* $[\![1,n]\!]$*, sur* $[\![1,n]\!]^k$ *et sur* $\mathcal{P}([\![1,n]\!])$*.*

(ii) $GL(E)$ *agit sur* E *et sur l'ensemble des sous-espaces vectoriels de* E*.*

(iii) $GL_n(\mathbb{K})$ *agit sur* $\mathbb{M}_n(\mathbb{K})$ *:* $(P, M) \in GL_n(\mathbb{K}) \times \mathbb{M}_n(\mathbb{K}) \longmapsto PMP^{-1}$*.*

V.2 Orbites et stabilisateurs

Définition 33.72 (Orbite)**.** *Si* G *agit sur* X*, l'*orbite *de* $x \in X$ *est :*

$$\omega_G(x) = \{g \cdot x,\ g \in G\}.$$

L'action est dite transitive *s'il n'y a qu'une seule orbite :* $\forall x \in X,\ \omega_G(x) = X$*.*

Définition 33.73 (Stabilisateur)**.** *Si G agit sur X, le* stabilisateur *de $x \in X$ est :*

$$G_x = \{g \in G,\ g \cdot x = x\}.$$

C'est un sous-groupe de G.

Proposition 33.74. *On a une bijection naturelle :*

$$\left| \begin{array}{c} G/G_x \longrightarrow \omega_G(x) \\ \overline{g} \longmapsto g \cdot x \end{array} \right. .$$

En particulier, si G est fini, $|G| = |\omega_G(x)| \cdot |G_x|$.

Lemme 33.75 (Lemme de Cauchy)**.** *G un groupe fini, $p \in \mathbb{P}$ t.q. $p \mid |G|$. Alors G contient un élément d'ordre p.*

Démonstration. Soit $X = \{(x_1, \ldots, x_p) \in G^p,\ x_1 \cdots x_p = e\}$. $\mathbb{Z}/p\mathbb{Z}$ agit sur X (par rotation des x_i). Et on a $|X| = |G|^{p-1} \equiv 0 \quad [p]$. De plus, les orbites de l'action de $\mathbb{Z}/p\mathbb{Z}$ sont de cardinal 1 ou p. Et l'orbite de $(x_1, \ldots, x_p)$ est de cardinal 1 ssi $x = x_1 = \cdots = x_p$, avec $x^p = e$. On note $N_p = |\{x \in G,\ x^p = e\}|$. On a donc $N_p \equiv 0 \quad [p]$. Le nombre d'éléments d'ordre p est donc $N_p - 1 \equiv -1 \quad [p]$ (car $p \in \mathbb{P}$), qui est donc non nul. □

VI Théorie de Galois des extensions finies (suite)

VI.1 Groupe de Galois d'un polynôme séparable

Notation 33.76. *Pour $\mathbb{P} \in \mathbb{K}[X]$, on note :*

$$\mathrm{Gal}_{\mathbb{K}}(P) = \mathrm{Gal}\left(D_{\mathbb{K}}(P)/\mathbb{K}\right).$$

Proposition 33.77. *$P = \prod_{i=1}^{n}(X - x_i) \in \mathbb{K}[X]$, où $(x_1, \ldots, x_n) \in \Omega^n$ deux à deux distincts. Alors l'action de $\mathrm{Gal}_{\mathbb{K}}(P)$ sur $\mathcal{R} = \{x_1, \ldots, x_n\}$ est fidèle, et elle est transitive* ssi *P est irréductible.*

Proposition 33.78. *$P = \prod_{i=1}^{n}(X - x_i) \in \mathbb{K}[X]$, où $(x_1, \ldots, x_n) \in \Omega^n$. On pose :*

$$\delta(P) = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i),$$

puis $\Delta(P) = \delta(P)^2$. Alors, en notant $\mathfrak{A}_{\mathcal{R}}$ le sous-groupe alterné de $\mathfrak{S}_{\mathcal{R}}$, avec $\mathcal{R} = (x_1, \ldots, x_n)$, on a :

$$\mathrm{Gal}_{\mathbb{K}}(P) \subset \mathfrak{A}_{\mathcal{R}} \Longleftrightarrow \delta(P) \in \mathbb{K}.$$

De plus, si $\delta(P) \notin \mathbb{K}$, alors $D_{\mathbb{K}}(P)^{\mathrm{Gal}_{\mathbb{K}}(P) \cap \mathfrak{A}_{\mathcal{R}}} = \mathbb{K}(\delta(P))$.

VII Sous-groupes normaux et groupes quotients

Notation 33.79. *G groupe, H sous-groupe de G. On note $G/H = \{\overline{a},\ a \in G\}$, avec $\overline{a} = aH$.*

Définition 33.80 (Sous-groupe normal)**.** *G groupe. On dit qu'un sous-groupe H de G est* normal *(ou* distingué*) dans G lorsque $\forall g \in G$, $\forall h \in H$, $ghg^{-1} \in H$. On écrit alors $H \triangleleft G$.*

Proposition 33.81. *Si $H \triangleleft G$, on peut définir une LCI sur G/H en posant $\overline{a} \cdot \overline{b} = \overline{ab}$, pour tout $(a,b) \in G^2$. L'ensemble G/H muni de cette loi est un groupe et l'application* $\begin{vmatrix} G \longrightarrow G/H \\ a \longmapsto \overline{a} \end{vmatrix}$ *est un morphisme de noyau H.*

Proposition 33.82. *G un groupe. Tout sous-groupe de G contenu dans $Z(G)$ est un sous-groupe normal de G.*

Proposition 33.83. *$\varphi : G \to H$ un morphisme de groupes. Alors* $\operatorname{Ker}\varphi \triangleleft G$ *et :*

$$G/\operatorname{Ker}\varphi \simeq \varphi(G).$$

Proposition 33.84. *$H \triangleleft G$. Les sous-groupes de G/H sont les K/H, avec K sous-groupe de G contenant H. De plus $(K/H) \triangleleft (G/H)$* ssi *$K \triangleleft G$.*

VIII Théorie de Galois des extensions finies (suite)

VIII.1 Second volet de la correspondance de Galois

Lemme 33.85. *$\mathbb{L}/\mathbb{K}$ une extension galoisienne finie. $\mathbb{K}' \in \mathcal{K}_{\mathbb{L}/\mathbb{K}}$, $\sigma \in \operatorname{Gal}(\mathbb{L}/\mathbb{K})$. Alors :*

$$\sigma \circ \operatorname{Gal}(\mathbb{L}/\mathbb{K}') \circ \sigma^{-1} = \operatorname{Gal}(\mathbb{L}/\sigma(\mathbb{K}')).$$

Démonstration. Montrer que $\mathbb{L}^{\sigma\circ\operatorname{Gal}(\mathbb{L}/\mathbb{K}')\circ\sigma^{-1}} = \sigma(\mathbb{K}')$. □

Théorème 33.86. *$\mathbb{L}/\mathbb{K}$ une extension galoisienne finie. $\mathbb{K}' \in \mathcal{K}_{\mathbb{L}/\mathbb{K}}$. Alors le sous-groupe* $\operatorname{Gal}(\mathbb{L}/\mathbb{K}')$ *est normal dans* $\operatorname{Gal}(\mathbb{L}/\mathbb{K})$ ssi *l'extension $\mathbb{K}'/\mathbb{K}$ est normale. Dans ce cas, on a :*

$$\operatorname{Gal}(\mathbb{L}/\mathbb{K})/\operatorname{Gal}(\mathbb{L}/\mathbb{K}') \simeq \operatorname{Gal}(\mathbb{K}'/\mathbb{K}).$$

IX Sous-groupes normaux et groupes quotients (suite)

IX.1 Groupes simples

Définition 33.87 (Groupe simple)**.** *Un groupe G est dit* simple *si ses seuls sous-groupes normaux sont $\{e\}$ et G.*

Proposition 33.88. *Si G est abélien et simple, alors $G \simeq \mathbb{Z}/p\mathbb{Z}$, avec $p \in \mathbb{P}$.*

Remarque 33.89. *Tout groupe fini G non nul admet un quotient simple (qui est donné par le sous-groupe normal maximal distinct de G).*

Théorème 33.90. *$\mathfrak{A}_5$ est simple.*

Démonstration. On utilise le fait que, pour un groupe G, $N \triangleleft G$ implique que N est une réunion de classes de conjugaison de G (les classes de conjugaison étant les $\{gh_0g^{-1},\ g \in G\}$, pour $h_0 \in G$). On va montrer qu'une réunion de classes de conjugaison de $\mathfrak{A}_5$ a un cardinal divisant $|\mathfrak{A}_5| = 60$ ssi elle est de cardinal 1 ou 60. On remarque d'abord que deux éléments de $\mathfrak{S}_n$ sont conjugués ssi ils ont le même type cyclique (le type cyclique de $\sigma \in \mathfrak{S}_n$ est le n-uplet $(\alpha_1(\sigma), \ldots, \alpha_n(\sigma))$, où $\alpha_i(\sigma)$ est le nombre de cycles de longueur i de σ). Montrer alors, pour $\sigma \in \mathfrak{S}_n$, que les classes de conjugaison de σ dans $\mathfrak{S}_n$ et $\mathfrak{A}_n$ sont les mêmes ssi il existe $\gamma \in \mathfrak{S}_n \backslash \mathfrak{A}_n$ commutant à σ ; sinon, la classe de conjugaison de σ dans $\mathfrak{S}_n$ est la réunion de deux classes de conjugaison équipotentes dans $\mathfrak{A}_n$. Montrer enfin que les classes de conjugaison dans $\mathfrak{A}_5$ sont de cardinal 1 (la classe de id), 20 (la classe des 3-cycles), 12 (les deux classes de 5-cycles dans $\mathfrak{A}_5$) et 15 (la classe des doubles transpositions). En déduire que toute réunion de classes de conjugaison de cardinal divisant 60 a pour cardinal 1 ou 60. □

IX.2 Suites de composition

Définition 33.91 (Suite de composition)**.** *G un groupe. Une* suite de composition *de G est une suite de sous-groupes*

$$\{e\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n = G,$$

avec $\forall i \in [\![1, n[\![$, $G_i \triangleleft G_{i+1}$. Les G_{i+1}/G_i sont dits quotients de la suite.

Vocabulaire 33.92. *G un groupe, $G_0, \ldots, G_n$ une suite de composition de G.*

(i) *La suite $G_0, \ldots, G_n$ est dite* normale *si $\forall i \in [\![1, n]\!]$, $G_i \triangleleft G$.*

(ii) *La suite $G_0, \ldots, G_n$ est dite* de Jordan-Hölder *si, pour tout $i \in [\![1, n[\![$, G_{i+1}/G_i est simple.*

Remarque 33.93. *Tout groupe fini admet une suite de Jordan-Hölder (car tout groupe fini non nul admet un quotient simple).*

IX.3 Groupe dérivé et abélianisé

Notation 33.94 (Commutateur)**.** *G un groupe. Pour $(x, y) \in G^2$, on note $[x, y] = xyx^{-1}y^{-1}$, dit* commutateur *de x et y.*

Définition 33.95 (Groupe dérivé)**.** *G un groupe. On note $D(G)$ (ou G') le sous-groupe de G, dit* sous-groupe dérivé de G*, engendré par les $[x, y]$, où $(x, y) \in G^2$.*

Définition 33.96 (Abélianisé)**.** *G un groupe. $D(G)$ est stable par tout automorphisme de G donc $D(G) \triangleleft G$. Le quotient $G/D(G)$ est appelé* abélianisé *de G.*

Proposition 33.97. *G un groupe. $N \triangleleft G$. Alors G/N est abélien* ssi *$D(G) \subset N$.*

IX.4 Groupes résolubles

Notation 33.98 (Dérivés successifs)**.** *G un groupe. On définit les* dérivés successifs *de G par $D^0(G) = G$ et $\forall n \in \mathbb{N}$, $D^{n+1}(G) = D\left(D^n(G)\right)$.*

Définition 33.99 (Groupes résolubles)**.** *On dit qu'un groupe G est* résoluble *lorsque :*

$$\exists n \in \mathbb{N},\ D^n(G) = \{e\}.$$

Proposition 33.100.

(i) *Si G est résoluble et H est un sous-groupe de G alors H est résoluble.*

(ii) *Si G_1 et G_2 sont résolubles alors $G_1 \times G_2$ l'est aussi.*

(iii) *Si G est résoluble et $N \triangleleft G$, alors G/N est résoluble.*

(iv) *Si G est résoluble et simple alors $G \simeq \mathbb{Z}/p\mathbb{Z}$, avec $p \in \mathbb{P}$.*

Démonstration. (i) $D(H) \subset D(G)$. (ii) $D\left(G_1 \times G_2\right) = D\left(G_1\right) \times D\left(G_2\right)$. (iii) Le quotient G/N est en fait l'image de G par le morphisme canonique $\varphi : G \to G/N$; or $\forall n \in \mathbb{N}$, $D^n\left(\varphi(G)\right) = \varphi\left(D^n(G)\right)$. (iv) $D(G) \triangleleft G$ et $D(G) \neq G$ (car G résoluble) et G simple donc $D(G) = \{e\}$. Donc $G \simeq G/D(G)$ est abélien et simple. □

Théorème 33.101. *G un groupe, $N \triangleleft G$. Alors :*

$$G \text{ est résoluble} \iff N \text{ et } G/N \text{ sont résolubles.}$$

Démonstration. ($\Rightarrow$) Clair avec la proposition 33.100. ($\Leftarrow$) Il existe $(r,s) \in \mathbb{N}^2$ t.q. $D^r(G/N) = \{e\}$ (donc $D^r(G) \subset N$; en effet, si $\varphi : G \to G/N$ est le morphisme canonique, on a $\varphi(D^r(G)) = D^r(\varphi(G)) = D^r(G/N) = \{e\}$, donc $D^r(G) \subset \operatorname{Ker}\varphi = N$) et $D^s(N) = \{e\}$. Ainsi, $D^{r+s}(G) = \{e\}$. □

Exemple 33.102.

(i) *$\mathfrak{S}_3$ et $\mathfrak{S}_4$ sont résolubles.*

(ii) *$D(\mathfrak{A}_5) = \mathfrak{A}_5$ donc $\mathfrak{A}_5$ n'est pas résoluble.*

(iii) *Pour $n \geqslant 5$, $\mathfrak{A}_5 \subset \mathfrak{S}_n$ donc $\mathfrak{S}_n$ n'est pas résoluble.*

Théorème 33.103. *G un groupe fini. Alors G est résoluble* ssi *G admet une suite de Jordan-Hölder à quotients cycliques d'ordres premiers.*

Démonstration. Utiliser le théorème 33.101. □

X Retour aux équations

X.1 Résolubilité par radicaux : condition nécessaire

Définition 33.104 (Extension résoluble par radicaux)**.** *On dit qu'une extension $\mathbb{L}/\mathbb{K}$ est* résoluble par radicaux *lorsqu'il existe*

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r,$$

avec $\mathbb{K} \subset \mathbb{L} \subset \mathbb{K}_r$ et $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha_i)$, où $\alpha_i^{n_i} \in \mathbb{K}_i$.

Lemme 33.105. *Si $\mathbb{L}/\mathbb{K}$ est une extension finie résoluble par radicaux alors le groupe $\operatorname{Gal}(\operatorname{Clnorm}_{\mathbb{K}}(\mathbb{L})/\mathbb{K})$ est résoluble.*

Démonstration. On notera $\mathbb{L}' = \operatorname{Clnorm}_{\mathbb{K}}(\mathbb{L})$. Montrer d'abord que $\mathbb{L}'/\mathbb{K}$ est résoluble par radicaux. Écrire $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_s$, avec $\mathbb{K} \subset \mathbb{L}' \subset \mathbb{K}_s$ et $\mathbb{K}_{i+1} = \mathbb{K}_i(\beta_i)$, où $\beta_i^{m_i} \in \mathbb{K}_i$. Poser alors $\mathbb{M} = \mathbb{K}_s = \mathbb{K}(\beta_0, \ldots, \beta_{s-1})$. En notant ε une racine primitive n-ième de 1, il suffit de montrer que $\operatorname{Gal}(\mathbb{M}(\varepsilon)/\mathbb{K})$ est résoluble pour en déduire que $\operatorname{Gal}(\mathbb{L}'/\mathbb{K})$ est résoluble. Comme l'extension $\mathbb{K}(\varepsilon)/\mathbb{K}$ est abélienne, il suffit pour cela de montrer que $\operatorname{Gal}(\mathbb{M}(\varepsilon)/\mathbb{K}(\varepsilon))$ est résoluble. On montre alors par récurrence descendante sur i que $\operatorname{Gal}(\mathbb{M}(\varepsilon)/\mathbb{K}_i(\varepsilon))$ est résoluble.

$$\begin{array}{ccccc} \mathbb{K} & \text{———} & \mathbb{L}' & \text{———} & \mathbb{M} \\ | & & | & & | \\ \mathbb{K}(\varepsilon) & \text{——} & \mathbb{L}'(\varepsilon) & \text{——} & \mathbb{M}(\varepsilon) \end{array}$$

□

X.2 Extensions cycliques de Kummer

Théorème 33.106. *$\mathbb{L}/\mathbb{K}$ une extension finie t.q. $|\mathbb{U}_n(\mathbb{K})| = n$. Alors les deux propriétés suivantes sont équivalentes :*

(i) $\exists a \in \mathbb{K}$, $\begin{cases} (X^n - a) \text{ est irréductible sur } \mathbb{K} \\ \mathbb{L} = D_{\mathbb{K}}(X^n - a) \end{cases}$,

(ii) $\operatorname{Gal}(\mathbb{L}/\mathbb{K}) \simeq \mathbb{Z}/n\mathbb{Z}$.

Démonstration. ($\Leftarrow$) Soit σ un générateur de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, ε une racine primitive n-ième de 1. *Première étape.* Il suffit de montrer que $\exists \alpha \in \mathbb{L}\backslash\{0\}$, $\sigma(\alpha) = \varepsilon\alpha$. En effet, si tel est le cas, les $\mathbb{K}$-conjugués de α seront les $\varepsilon^k\alpha$, $k \in [\![0, n[\![$, donc $\Pi_{\mathbb{K},\alpha} = X^n - a$, avec $a = \alpha^n$. Et $[\mathbb{K}(a) : \mathbb{K}] = n$, $[\mathbb{L} : \mathbb{K}] = n$, avec $\mathbb{K}(a) \subset \mathbb{L}$, d'où $\mathbb{L} = \mathbb{K}(a) = D_{\mathbb{K}}(X^n - a)$. *Deuxième étape.* Noter que $(X^n - 1)$ annule σ, et les σ^k, $k \in [\![0, n[\![$ sont libres. Donc $(X^n - 1)$ est le polynôme minimal de σ. Les racines de $(X^n - 1)$ sont donc les valeurs propres de σ, d'où l'existence de α. □

X.3 Résolubilité par radicaux : condition suffisante

Théorème 33.107. *Soit $\mathbb{L}/\mathbb{K}$ une extension finie, avec $\mathbb{K}$ de caractéristique nulle. Alors l'extension $\mathbb{L}/\mathbb{K}$ est résoluble par radicaux* ssi *le groupe* $\mathrm{Gal}\left(\mathrm{Clnorm}_{\mathbb{K}}(\mathbb{L})/\mathbb{K}\right)$ *est résoluble.*

Démonstration. ($\Rightarrow$) Lemme 33.105. ($\Leftarrow$) Soit $G = \mathrm{Gal}(\mathbb{L}'/\mathbb{K})$, avec $\mathbb{L}' = \mathrm{Clnorm}_{\mathbb{K}}(\mathbb{L})$. On suppose G résoluble : $G = G_r \supset G_{r-1} \supset \cdots \supset G_0 = \{e\}$, avec $G_i \triangleleft G_{i+1}$ et G_{i+1}/G_i cyclique de cardinal premier. Par la correspondance de Galois : $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r = \mathbb{L}'$, où $\mathbb{K}_i = \mathbb{L}'^{G_{r-i}}$. Soit ε une racine primitive n-ième de 1. Noter que $\mathbb{K}_{i+1}/\mathbb{K}_i$ est normale, et $\mathrm{Gal}(\mathbb{K}_{i+1}/\mathbb{K}_i) \simeq \mathbb{Z}/p_i\mathbb{Z}$, $p_i \in \mathbb{P}$. Par irrationalité naturelle (théorème 33.64), $\mathbb{K}_{i+1}(\varepsilon)/\mathbb{K}_i(\varepsilon)$ est normale, et son groupe de Galois est nul ou cyclique de cardinal p_i. Donc par Kummer (théorème 33.106), $\mathbb{K}_{i+1}(\varepsilon) = \mathbb{K}_i(\alpha_i, \varepsilon)$, où $\alpha_i^{p_i} \in \mathbb{K}_i(\varepsilon)$. Donc $\mathbb{L}'(\varepsilon)/\mathbb{K}$ est résoluble ; et $\mathbb{L}/\mathbb{K}$ aussi. □