Résumé de cours :
Semaine 24, du 24 au 28 mars.

Équations différentielles (fin)

1 Equations à variables séparées

Notation.
Soient I et K deux intervalles infinis et soient $a : I \longrightarrow \mathbb{R}$ et $b : K \longrightarrow \mathbb{R}$ deux applications continues.
L'équation différentielle $(E)\ :\ a(t) - b(y)y' = 0$ est appelée une équation est à variables séparées.
Si A et B sont des primitives de a et de b respectivement,
$(E) \Longleftrightarrow \dfrac{d\big(A(t) - B(y(t))\big)}{dt} = 0$, donc les courbes intégrales de (E) ont pour équations cartésiennes $A(x) = B(y) + C$, où $C \in \mathbb{R}$.
En pratique, on écrira $(E) \Longleftrightarrow a(t)dt = b(y)dy \Longleftrightarrow A(t) = B(y) + C$.

2 Equations à variables séparables

Notation. Soient I et K deux intervalles infinis. Soient a et d deux applications continues de I dans $\mathbb{R}$ et b et c deux applications continues de K dans $\mathbb{R}$. L'équation $(E)\ :\ a(t)c(y) - b(y)d(t)y' = 0$ est appelée une équation est à variables séparables.
En divisant par $c(y)$ et $d(t)$ on se ramene à une équation à variables séparées.
• Plus précisément, soit $y : I \longrightarrow \mathbb{R}$ une application dérivable. Quitte à restreindre l'intervalle I, on supposera que d ne s'annule pas sur I. Ainsi $(E) \Longleftrightarrow \dfrac{a(t)}{d(t)}c(y) - y'b(y) = 0$.
Il faudra ensuite étudier les possibles raccordements des solutions en chaque zéro de d.
• Si $y_0 \in K$ est un zéro de c, l'application constante $y = y_0$ est une solution de (E). Ainsi chaque zéro de c fournit une solution particulière.
On suppose ensuite que $\forall t \in I\ \ c(y(t)) \neq 0$. Alors $(E) \Longleftrightarrow \dfrac{a(t)}{d(t)} - y'\dfrac{b(y)}{c(y)} = 0$: c'est une équation à variables séparées, donc on est ramené au a). Il reste ensuite à étudier les possibles recollements de ces dernières solutions avec les solutions particulières $y = y_0$ où y_0 est un zéro de c.

Les polynômes (début)

3 Le groupe des polynômes

Notation. A désigne un anneau quelconque.

Définition. On note $A[X] \triangleq A^{(\mathbb{N})}$: c'est l'ensemble des suites presque nulles.

Si $P = (a_k) \in A[X]$, on convient de noter $P = \sum_{k \in \mathbb{N}} a_k X^k$.

Remarque. Par définition, deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients.

Propriété. Si $P(X) = \sum_{k \in \mathbb{N}} a_k X^k$ et $Q(X) = \sum_{k \in \mathbb{N}} b_k X^k$, alors $P + Q = \sum_{k \in \mathbb{N}} (a_k + b_k) X^k$.
$(A[X], +)$ est un sous-groupe commutatif de $A^{\mathbb{N}}$ dont le neutre est le polynôme identiquement nul.

Définition. Si $P(X) = (a_k)_{k \in \mathbb{N}} \in A[X] \setminus \{0\}$, $\deg(P) = \max(\{k \in \mathbb{N}/a_k \neq 0\})$.
On convient que $\deg(0) = -\infty$.

Définition. Soit $P(X) = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$ un polynôme de degré $n \in \mathbb{N}$.

- a_k est le coefficient de P de degré k.
- a_0 est aussi appelé le coefficient constant du polynôme P.
- a_n est appelé le coefficient de plus haut degré de P, ou bien son coefficient dominant.
- On dit que P est unitaire (ou normalisé) si et seulement si $a_n = 1$.
- Le polynôme $a_k X^k$ est appelé un monôme.

Notation. Pour tout $n \in \mathbb{N}$, on note $A_n[X] = \{P \in A[X]/\deg(P) \leq n\}$. Ainsi, $A[X] = \bigcup_{n \in \mathbb{N}} A_n[X]$.

Propriété. $\deg(P + Q) \leq \sup(\deg(P), \deg(Q))$, avec égalité lorsque $\deg(P) \neq \deg(Q)$.

4 Produits de polynômes

Définition. $\left(\sum_{n \in \mathbb{N}} a_n X^n\right) \times \left(\sum_{n \in \mathbb{N}} b_n X^n\right) \triangleq \sum_{n \in \mathbb{N}} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) X^n$.

Propriété. Pour tout $P, Q \in A[X]$, PQ est aussi un élément de $A[X]$.

Propriété. $(A[X], +, \times)$ est un anneau, avec $1_{A[X]} = (\delta_{k,0} 1_A)_{k \in \mathbb{N}}$.

Remarque. $\left(\sum_{n \in \mathbb{N}} a_n X^n\right) \times \left(\sum_{n \in \mathbb{N}} b_n X^n\right) \times \left(\sum_{n \in \mathbb{N}} c_n X^n\right) = \sum_{n \in \mathbb{N}} \Big(\sum_{\substack{(i,j,k) \in \mathbb{N}^3 \\ i+j+k=n}} a_i b_j c_k\Big) X^n$.

Propriété. L'application $\begin{array}{rccl} i: & A & \longrightarrow & A[X] \\ & a & \longmapsto & (a\delta_{0,k})_{k \in \mathbb{N}} \end{array}$ est un morphisme injectif d'anneaux. On identifie A avec une partie de $A[X]$ en convenant que, pour tout $a \in a$, $a = i(a)$. Alors $A_0[X] = A$.

Remarque. Lorsque $b \in A$ et $P \in A[X]$, on dispose donc du produit bP.
Si $P = \sum_{k \in \mathbb{N}} a_k X^k$, on vérifie que $bP = \sum_{k \in \mathbb{N}} b a_k X^k$.

Propriété. $A[X]$ est commutatif intègre si et seulement si A est commutatif intègre.
Il faut savoir le démontrer.

Pour toute la suite de ce chapitre, on supposera que A est commutatif intègre.

Propriété. Pour tout $P, Q \in A[X]$, $\deg(PQ) = \deg(P) + \deg(Q)$.
Il faut savoir le démontrer.

Propriété. $U(A[X]) = U(A)$.
Il faut savoir le démontrer.

Définition. L'indéterminée X est le polynôme $(1_A \delta_{k,1})_{k\in\mathbb{N}}$. On a $X^n = (1_A \delta_{k,n})_{k\in\mathbb{N}}$.

5 Polynômes à plusieurs indéterminées (hors programme)

A est commutatif intègre, donc $A[X]$ est commutatif intègre, puis $(A[X])[Y]$ est aussi un anneau commutatif intègre. Ce dernier ensemble est l'anneau des polynômes à deux indéterminées à coefficients dans A. On le note plutôt $A[X, Y]$.
Il est isomorphe à $A^{(\mathbb{N}^2)}$, en convenant que $(a_{h,k})_{(h,k)\in\mathbb{N}^2} = \displaystyle\sum_{\substack{0\le h\le m\\ 0\le k\le n}} a_{h,k} X^h Y^k$.
Dans ces conditions, $\boxed{X = (\delta_{h,1}\delta_{k,0})_{(h,k)\in\mathbb{N}^2} \text{ et } Y = (\delta_{h,0}\delta_{k,1})}$.
On peut vérifier que, pour tout $p, q \in \mathbb{N}^2$, $X^p Y^q = (\delta_{h,p}\delta_{k,q})_{(h,k)\in\mathbb{N}^2}$.
En généralisant, on peut définir $A[X_1, \dots, X_p]$, l'anneau des polynômes à p indéterminées.

6 Applications polynomiales

Définition. Soit $P = \displaystyle\sum_{k\in\mathbb{N}} a_k X^k \in A[X]$ un polynôme. L'application polynomiale associée à P est l'application $\begin{array}{rccl} \tilde{P}: & A & \longrightarrow & A \\ & x & \longmapsto & \displaystyle\sum_{k\in\mathbb{N}} a_k x^k \end{array}$.

Propriété. L'application $\begin{array}{rccl} \varphi: & A[X] & \longrightarrow & \mathcal{F}(A, A) \\ & P & \longmapsto & \tilde{P} \end{array}$ est un morphisme d'anneaux.

Notation. $Im(\varphi)$ est un sous-anneau de $\mathcal{F}(A, A)$. C'est l'anneau des applications polynomiales.

Théorème. Lorsque A est un corps, φ est injectif si et seulement si A est de cardinal infini.

Algorithme d'Hörner : Soit $P = \displaystyle\sum_{k\in\mathbb{N}} a_k X^k \in A[X]$ et $x \in A$. On peut disposer le calcul de $\tilde{P}(x)$ de la manière suivante : $\tilde{P}(x) = (\cdots((a_n x + a_{n-1})x + a_{n-2}x) + \cdots + a_1)x + a_0$. Cet algorithme permet de calculer $\tilde{P}(x)$ avec n multiplications et n additions.

7 Composition de polynômes

Définition. Si $P = \displaystyle\sum_{k=0}^{n} a_k X^k \in A[X]$ et $Q \in A[X]$, $P \circ Q = \displaystyle\sum_{k=0}^{n} a_k Q^k = P(Q)$.

Propriété. Pour tout $P, Q, R \in A[X]$,
- $(P + Q) \circ R = P \circ R + Q \circ R$,
- $(PQ) \circ R = (P \circ R) \times (Q \circ R)$,
- $(P \circ Q) \circ R = P \circ (Q \circ R)$.

Propriété. Soit $P, Q \in A[X]$ Si $\deg(Q) \ge 1$, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.
Il faut savoir le démontrer.

Propriété. Pour tout $P, Q \in A[X]$, $\widetilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$.

8 Dérivation formelle

Définition. Si $P = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$, on pose $P' \triangleq \sum_{k\in\mathbb{N}^*} k a_k X^{k-1} = \sum_{k\in\mathbb{N}} (k+1) a_{k+1} X^k$.

Remarque. On peut écrire $P' = \sum_{k\in\mathbb{N}} k a_k X^{k+1}$, si l'on convient que $0X^{-1} = 0$.

Définition. Si $P = \sum_{k\in\mathbb{N}} a_k X^k$, $P^{(0)} = P$ et

pour tout $n \in \mathbb{N}$, $P^{(n)} = \sum_{k\geq n} \frac{k!}{(k-n)!} a_k X^{k-n} = \sum_{k\in\mathbb{N}} \frac{(k+n)!}{k!} a_{k+n} X^k$.

Propriété. Pour tout $P \in \mathbb{R}[X]$ et $n \in \mathbb{N}$, $\widetilde{P^{(n)}} = \tilde{P}^{(n)}$.

Propriété. Pour tout $P \in A[X]$, $\deg(P') \leq \deg(P) - 1$.

Propriété. Pour tout $P \in A[X] \setminus \{0\}$, $P^{(\deg(P)+1)} = 0$.

Propriété. Soit $P, Q \in A[X]$, $a \in A$ et $n \in \mathbb{N}$.
- $(P+Q)' = P' + Q'$, et plus généralement, $(P+Q)^{(n)} = P^{(n)} + Q^{(n)}$.
- $(aP)' = aP'$, et plus généralement, $(aP)^{(n)} = aP^{(n)}$.
- $(PQ)' = P'Q + PQ'$

Propriété. Pour tout $n \in \mathbb{N}$ et $P_1, \ldots, P_n \in A[X]$, $(P_1 \times \cdots \times P_n)' = \sum_{i=1}^{n} P_i' \prod_{j\neq i} P_j$.

Formule de Leibniz : $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Propriété. Pour tout $P, Q \in A[X]$, $(P \circ Q)' = Q' \times (P' \circ Q)$.

9 La structure d'algèbre de $\mathbb{K}[X]$.

Pour la suite de ce chapitre, $\mathbb{K}$ désigne un corps.

Propriété. $\mathbb{K}[X]$ est une $\mathbb{K}$-algèbre.

Propriété. La base canonique de $\mathbb{K}[X]$ est la famille $(X^n)_{n\in\mathbb{N}}$.

Propriété. Soit $n \in \mathbb{N}$. $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ dont une base est $(1, X, \ldots, X^n)$, encore appelée la base canonique de $\mathbb{K}_n[X]$. On en déduit que $\dim(\mathbb{K}_n[X]) = n + 1$.

> **Exercice.** Soit $(P_n)_{n\in\mathbb{N}}$ une suite de polynômes de $\mathbb{K}[X]$. On suppose que cette suite de polynômes est étagée c'est-à-dire que, $\forall n \in \mathbb{N} \quad \deg(P_n) = n$.
> Montrer que pour tout $N \in \mathbb{N}$, $(P_n)_{0\leq n\leq N}$ est une base de $\mathbb{K}_N[X]$.
> En déduire que $(P_n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$.
> Il faut savoir le démontrer.

10 Division euclidienne entre polynômes

Théorème. Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple $(P, Q) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$: Q est le quotient de la division euclidienne du dividende A par le diviseur B et que R en est le reste.
Il faut savoir le démontrer.

Définition. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est une racine de A si et seulement si $\tilde{A}(a) = 0$.

Propriété. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le reste de la division euclidienne de A par $X - a$ est égal au polynôme constant $\tilde{A}(a)$.
Il faut savoir le démontrer.

Corollaire. a est racine de A si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $A = (X - a)Q$.

Propriété. Supposons que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$. Alors, pour tout $(A, B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$, les quotient et reste de la division euclidienne sont les mêmes que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

11 Arithmétique

11.1 Divisibilité

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$. $a|b$ si et seulement si $\exists m \in A \ \ b = ma$.
On dit alors que a est un ***diviseur*** de b et que b est un ***multiple*** de a.

Remarque. $0|a \iff a = 0$ et, pour tout $a \in A$, $a|0$.

Propriété. Soit $P, Q \in \mathbb{K}[X]$ tels que $P \mid Q$ et $Q \neq 0$. Alors $\deg(Q) \geq \deg(P)$.

Propriété. Soit $P, Q \in \mathbb{K}[X]$ avec $Q \neq 0$. $P \mid Q$ si et seulement si le reste de la divison euclidienne de P par Q est nul.

Propriété. Soit $\mathbb{L}$ un sous-corps d'un corps $\mathbb{K}$. Soit $P, Q \in \mathbb{L}[X]$.
Alors $P \mid Q$ dans $\mathbb{L}[X]$ si et seulement si $P \mid Q$ dans $\mathbb{K}[X]$.
Il faut savoir le démontrer.

Propriété. Soient A un anneau commutatif et $a, b, c, d \in A$.
— Si $b \mid a$ et $b \mid c$, alors $b \mid (a + c)$.
— Si $b \mid a$ et $d \mid c$, alors $bd \mid ac$.
— si $b \mid a$, pour tout $p \in \mathbb{N}$, $b^p \mid a^p$.

Propriété. Soient A un anneau commutatif et $b, a_1, \ldots, a_p, c_1, \ldots, c_p \in A$.
Si pour tout $i \in \{1, \ldots, p\}$, $b \mid a_i$, alors $b \mid \sum_{i=1}^{p} c_i a_i$.

Propriété. Soient A un anneau commutatif et $(a, b) \in A^2$. $a|b \iff bA \subseteq aA$.

Propriété. Soit A un anneau commutatif. La relation de divisibilité est réflexive et transitive.

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$.
a et b sont ***associés*** si et seulement si $a|b$ et $b|a$.
La relation "être associé à" est une relation d'équivalence, on la notera "$\sim$".

Propriété. Dans un anneau commutatif, si $a \sim b$ et $c \sim d$, alors $ac \sim bd$.

Hypothèse : Jusqu'à la fin de ce paragraphe, on suppose que A est intègre et commutatif.

Propriété. Soit $a, b \in A$. a et b sont associés si et seulement s'il existe $\lambda \in U(A)$ tel que $a = \lambda b$.
Il faut savoir le démontrer.

Exemple. Dans $\mathbb{Z}$, n et m sont associés si et seulement si $|n| = |m|$.
Dans $\mathbb{K}[X]$, P et Q sont associés si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.

Propriété. La relation de divisibilité est une relation d'ordre sur $\mathbb{N}$.
La relation de divisibilité est une relation d'ordre sur l'ensemble des polynômes unitaires de $\mathbb{K}[X]$.

Définition. Soit $p \in A$. p est irréductible dans A si et seulement si $p \notin U(A)$ et si, pour tout $a, b \in A$, $p = ab \Longrightarrow (a \in U(A)) \vee (b \in U(A))$.
Ainsi p est irréductible dans A si et seulement si p n'est pas inversible et a pour seuls diviseurs les éléments associés à 1 ou à p.

Remarque. Si p est irréductible, il est non nul.

Propriété. Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.

Exemple. Dans $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps), un polynôme P est irréductible si et seulement si il est de degré supérieur ou égal à 1 et si, pour tout $A, B \in \mathbb{K}[X]$, $P = AB \Longrightarrow (\deg(A) = 0) \vee (\deg(B) = 0)$.

Remarque. Dans $\mathbb{K}[X]$:
- tout polynôme de degré 1 est irréductible ;
- tout polynôme de degré ≥ 2 possédant une racine dans $\mathbb{K}$ est réductible ;
- tout polynôme de degré 2 ou 3 sans racine dans $\mathbb{K}$ est irréductible.

Il faut savoir le démontrer.

Définition. Soit $a, b \in A$. On dit que a et b sont premiers entre eux (ou étrangers) si et seulement si les seuls diviseurs communs de a et b sont les éléments inversibles.

Définition. Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \ldots, a_n \in A$.
- $a_1, \ldots, a_n$ sont deux à deux premiers entre eux si et seulement si, pour tout $i, j \in \{1, \ldots, n\}$ avec $i \neq j$, a_i et a_j sont premiers entre eux.
- $a_1, \ldots, a_n$ sont globalement premiers entre eux si et seulement si les seuls diviseurs communs de $a_1, \ldots, a_n$ sont les éléments inversibles de A.

Propriété. Soit $p \in A$ un élément irréductible et $a \in A$: $p | a$, ou bien p et a sont premiers entre eux.
Il faut savoir le démontrer.

11.2 PGCD

Théorème. Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est un anneau principal.
Il faut savoir le démontrer.

Notation. Jusqu'à la fin de ce chapitre "arithmétique", on fixe un anneau A que l'on suppose principal.

Définition. Soit $(a, b) \in A^2$. d est un PGCD de a et b si et seulement si $aA + bA = dA$.

Caractérisation du PGCD par divisibilité : d est un PGCD de $(a, b) \in A^2$ si et seulement si d est un diviseur commun de a et b et si, pour tout diviseur commun d' de a et b, d' divise d.
Il faut savoir le démontrer.

Propriété. a et b sont premiers entre eux si et seulement si 1 est un PGCD de a et b.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \ldots, a_k \in A$, on dit que d est un PGCD de $a_1, \ldots, a_k$ si et seulement si $dA = a_1 A + \cdots + a_k A$, i.e si et seulement si d est un commun diviseur de $a_1, \ldots, a_k$ tel que si d' est un autre commun diviseur de $a_1, \ldots, a_k$, alors d' divise d.
Soit B une partie quelconque de A. d est un PGCD de B si et seulement si $dA = Id(B)$, i.e si et seulement si d est un diviseur commun des éléments de B tel que si d' est un autre diviseur commun des éléments de B, alors d' divise d.

Propriété. Lorsque $A = \mathbb{Z}$ (resp : $A = \mathbb{K}[X]$), en imposant au PGCD d'être positif (resp : unitaire) il est unique. On le note alors $a \wedge b$.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \ldots, a_k \in A$ et $h \in \{1, \ldots, k\}$.
Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,

— Commutativité du PGCD :
pour tout $\sigma \in \mathcal{S}_k$, $PGCD(a_1, \ldots, a_k) \sim PGCD(a_{\sigma(1)}, \ldots, a_{\sigma(k)})$.
— Associativité du PGCD :
$PGCD(a_1, \ldots, a_k) \sim PGCD(PGCD(a_1, \ldots, a_h), PGCD(a_{h+1}, \ldots, a_k))$.
— Distributivité de la multiplication par rapport au PGCD : pour tout $\alpha \in A$,
$PGCD(\alpha a_1, \ldots, \alpha a_k) \sim \alpha PGCD(a_1, \ldots, a_k)$.

Il faut savoir le démontrer.

11.3 PPCM

Définition. Soit $(a, b) \in A^2$. m est un PPCM de a et b si et seulement si $aA \cap bA = mA$.

Caractérisation du PPCM par divisibilité : m est un PPCM de $(a, b) \in A^2$ si et seulement si m est un multiple commun de a et b et si, pour tout multiple commun m' de a et b, m' est un multiple de m.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \ldots, a_k \in A$, m est un PPCM de $a_1, \ldots, a_k$ si et seulement si $mA = a_1A \cap \cdots \cap a_kA$, i.e si et seulement si m est un commun multiple de $a_1, \ldots, a_k$ tel que si m' est un autre commun multiple de $a_1, \ldots, a_k$, alors m' est un multiple de m.
Soit B est une partie quelconque de A. m est un PPCM de B si et seulement si $mA = \bigcap_{b \in B} bA$, i.e si et seulement si m est un multiple commun des éléments de B tel que si m' est un autre multiple commun des éléments de B, alors m' est un multiple commun de m.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \ldots, a_k \in A$ et $h \in \{1, \ldots, k\}$.
Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,
— Commutativité du PPCM :
pour tout $\sigma \in \mathcal{S}_k$, $PPCM(a_1, \ldots, a_k) \sim PPCM(a_{\sigma(1)}, \ldots, a_{\sigma(k)})$.
— Associativité du PPCM :
$PPCM(a_1, \ldots, a_k) \sim PPCM(PPCM(a_1, \ldots, a_h), PPCM(a_{h+1}, \ldots, a_k))$.
— Distributivité de la multiplication par rapport au PPCM :
pour tout $\alpha \in A$, $PPCM(\alpha a_1, \ldots, \alpha a_k) \sim \alpha PPCM(a_1, \ldots, a_k)$.