Algèbre différentielle

Lecture dirigée : Eliot Hecky et Gabriel Bartlett

Introduction

Développée par Ritt et Kolchin au vingtième siècle, l'algèbre différentielle a pour objet l'étude des propriétés algébriques des équations différentielles. Elle apporte un point de vue nouveau sur leur étude, en s'intéressant moins aux propriétés analytiques des solutions qu'aux propriétés algébriques des équations. L'étude portera en premier lieu sur de l'algèbre générale avec pour but le théorème de la base de Hilbert, qui motivera la seconde partie où seront étudiés les anneaux différentiels et leurs idéaux, afin de terminer sur le théorème de Ritt-Raudenbush et ses conséquences.

1 Anneaux noethériens

1.1 Définitions

Définition 1 *(anneau).* Un anneau est un ensemble A muni de deux lois de compositions internes $+$ et $\times$ telles que :
- $(A, +)$ est un groupe abélien ;
- $\times$ est associative et admet un élément neutre noté 1_A ;
- $\times$ est distributive par rapport à $+$;
- $\times$ est commutative.

◇ Remarque. Les anneaux sont donc (ici) commutatifs et unitaires. Dans la suite, on écrira A au lieu de $(A, +, \times)$ si les lois ne sont pas ambiguës. Sauf mention contraire, pour tous $x, y \in A$, leur composition par la première loi sera notée $x + y$ et leur composition par la seconde sera notée xy.

Exemple 2. Les ensembles $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ munis des lois $+$ et $\times$ usuelles forment quatre anneaux.

Définition 3 *(idéal).* Soit A un anneau. On dit qu'une partie $I \subset A$ est un idéal de A si :
- I est un sous-groupe de $(A, +)$;
- pour tous $x \in I$ et $y \in A$, $xy \in I$.

Exemple 4. Soit $n \in \mathbf{N}$. L'ensemble $n\mathbf{Z}$ forme un idéal de l'anneau $\mathbf{Z}$. En effet, il s'agit bien d'un sous-groupe de $(\mathbf{Z}, +)$ et tout produit d'un entier par un multiple de n est un multiple de n.

Réciproquement, tout idéal I de $\mathbf{Z}$ est un sous-groupe de $(\mathbf{Z}, +)$, donc $I = n\mathbf{Z}$ pour un certain $n \in \mathbf{N}$.

Exemple 5. Le sous-anneau $\mathbf{Q}$ de $\mathbf{R}$ n'en est pas un idéal car $1 \times \sqrt{2} \notin \mathbf{Q}$, pourtant 1 est rationnel.

PROPOSITION 6. Une intersection d'idéaux est un idéal.

Démonstration : Soient A un anneau et $(I_j)_{j\in J}$ une famille d'idéaux de A. On pose $I \overset{\text{def}}{=} \bigcap_{j\in J} I_j$. Alors I est un sous-groupe de $(A,+)$. Soient $x \in I$ et $y \in A$. Pour tout $j \in J$, $x \in I_j$ donc $xy \in I_j$. Finalement, $xy \in I$. □

PROPOSITION 7. La réunion d'une suite *croissante* d'idéaux est un idéal.

Démonstration : Soient A un anneau et $(I_n)_{n\in\mathbf{N}}$ une suite d'idéaux de A, croissante pour l'inclusion. On pose $I \overset{\text{def}}{=} \bigcup_{n\in\mathbf{N}} I_n$. C'est une réunion croissante de sous-groupes de $(A,+)$ donc c'est un sous-groupe de $(A,+)$. De plus, pour tous $x \in I$ et $y \in A$, il existe $n \in \mathbf{N}$ tel que $x \in I_n$, donc $xy \in I_n \subset I$. Cela démontre que I est un idéal de A. □

DÉFINITION 8 *(idéal engendré).* Soient A un anneau et $B \subset A$. L'idéal engendré par B, noté (B), est l'idéal minimal pour l'inclusion parmi les idéaux de A contenant B. C'est l'intersection de tous les idéaux contenant B.

PROPOSITION 9. Soient A un anneau et $B \subset A$. Alors (B) est l'ensemble des combinaisons linéaires à coefficients dans A d'éléments de B.

DÉFINITION 10 *(idéal premier).* Soit A un anneau. On dit qu'un idéal I de A est premier s'il est différent de A et si pour tous $x, y \in A$ tels que $xy \in I$, l'un des deux éléments x ou y appartient à I.

EXEMPLE 11. Soit p un nombre premier. Alors $p\mathbf{Z}$ est un idéal premier de $\mathbf{Z}$, puisque d'après le lemme d'Euclide, si p divise un produit d'entiers ab alors p divise a ou b.

D'autre part, si $a, b \geqslant 2$, alors $ab\mathbf{Z}$ n'est pas un idéal premier de $\mathbf{Z}$. En effet, $a \times b \in ab\mathbf{Z}$ pourtant ni a ni b n'appartiennent à $ab\mathbf{Z}$.

DÉFINITION 12 *(idéal maximal).* Soit A un anneau. On dit qu'un idéal I de A est maximal s'il est différent de A et si tout idéal de A contenant I est soit I, soit A.

PROPOSITION 13. Tout idéal maximal d'un anneau est aussi un idéal premier.

Démonstration : Soient A un anneau et I un idéal maximal de A. Soient aussi $x, y \in A$ tels que $xy \in I$. Supposons que $x \notin I$ et montrons que $y \in I$.

Comme $x \notin I$, l'idéal (I, x) engendré par $I \cup \{x\}$ contient I et est différent de I, donc $(I, x) = A$ par maximalité. Il contient donc 1_A, ce qui veut dire qu'il existe $z \in I$ et $w \in A$ tels que $1 = z + wx$. Ainsi :

$$y = yz + wxy \in I$$

car $z \in I$ et $xy \in I$. □

Définition 14 *(anneau intègre).* On dit qu'un anneau A est intègre s'il est non nul et s'il ne possède aucun diviseur de zéro, c'est-à-dire si pour tous $x, y \in A$ tels que $xy = 0_A$, l'un des deux éléments x ou y est nul.

Exemple 15. L'anneau $\mathbf{C}$ des nombres complexes est intègre, mais l'anneau $\mathbf{Z}/6\mathbf{Z}$ des entiers modulo 6 n'est pas intègre, puisque dans $\mathbf{Z}/6\mathbf{Z}$, l'identité $2 \times 3 = 0$ est vraie.

Définition 16 *(élément irréductible).* Soit A un anneau intègre. On dit qu'un élément $x \in A$ est irréductible s'il n'est pas inversible et si pour tous $y, z \in A$ tels que $x = yz$, l'un des deux éléments y ou z est inversible.

Définition 17 *(anneau factoriel).* On dit qu'un anneau intègre A est factoriel si :

— pour tout $x \in A$ non nul, il existe une famille $(p_i)_{1 \leqslant i \leqslant r}$ d'éléments irréductibles de A telle que :
$$x = \prod_{i=1}^{r} p_i \ ;$$

— pour tout élément non nul de A admettant deux factorisations $\prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j$, les nombres r et s sont égaux et l'on dispose d'une permutation $\sigma \in \mathfrak{S}_r$ ainsi que d'une famille $(u_i)_{1 \leqslant i \leqslant r}$ d'éléments inversibles de A tels que pour tout $i \in [\![1, r]\!]$:
$$p_i = u_i q_{\sigma(i)}.$$

Définition 18 *(idéal principal).* Soit A un anneau. On dit qu'un idéal I de A est principal s'il est engendré par un singleton.

Définition 19 *(anneau principal).* On dit qu'un anneau A est principal si tous ses idéaux sont principaux.

Exemple 20. L'anneau $\mathbf{R}[X]$ des polynômes à coefficients réels en une indéterminée est principal.

En effet, soit I un idéal de $\mathbf{R}[X]$. Supposons que $I \neq \{0\}$ (sinon, c'est évident). L'ensemble formé des degrés des polynômes non nuls de I est une partie non vide de $\mathbf{N}$; soit donc P un polynôme non nul de degré minimal dans I. Alors pour tout $Q \in I$, on dispose, par division euclidienne, de $S, R \in \mathbf{R}[X]$ avec $\deg(R) < \deg(P)$ tels que :
$$Q = SP + R$$
Mais alors $SP \in I$ donc $Q - SP \in I$, donc $R \in I$. Sauf que $\deg(R) < \deg(P)$, donc R est nul (par minimalité de $\deg(P)$) et $Q = SP$. Finalement, I est engendré par le polynôme P, ce qui démontre la principalité de $\mathbf{R}[X]$.

Exemple 21. L'anneau $\mathbf{Z}[X]$ des polynômes à coefficients entiers en une indéterminée n'est pas principal.

En effet, soit $I = (2, X)$ l'idéal engendré par 2 et X. Si cet idéal était principal il serait

engendré par un polynôme P de degré nul (puisque $2 \in I$ doit être divisible par P). Donc $P \in \mathbf{Z}$. De plus $X \in I$ donc X est un multiple de P, ce qui montre que $P \in \{-1, 1\}$. Sauf que dans ce cas, $I = \mathbf{Z}[X]$, ce qui est impossible puisque $1 \notin I$.

En conclusion, I n'est pas un idéal principal, donc $\mathbf{Z}[X]$ n'est pas un anneau principal.

DÉFINITION 22 *(pgcd).* Soient A un anneau et $(a_i)_{i\in I}$ une famille d'éléments de A. On dit qu'un élément d de A est un pgcd des a_i si pour tout $i \in I$, $d \mid a_i$ et si pour tout $d' \in A$ vérifiant cette propriété, $d' \mid d$.

PROPOSITION 23. Soient A un anneau intègre principal et $a, b \in A$ des éléments non nuls. Alors pour tout $c \in A$ engendrant l'idéal (a, b), c est un pgcd de a et b.

Démonstration : Comme $(a, b) = (c)$, c divise à la fois a et b. De plus, si $d \in A$ est un diviseur de a et de b, on dispose de $a', b' \in A$ tels que $a = da'$ et $b = db'$. Comme $c \in (a, b)$, on dispose aussi de $x, y \in A$ tels que :

$$c = xa + yb = xda' + ydb' = d(xa' + yb')$$

ce qui démontre que d divise c. □

LEMME 24 *(d'Euclide).* Soient A un anneau intègre principal et $p \in A$ irréductible. Si $a, b \in A$ sont tels que $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration : Si $p \nmid a$ alors (p, a) est engendré par un pgcd de p et a qui est nécessairement inversible, donc 1 engendre (p, a) et on dispose de $x, y \in A$ tels que :

$$1 = xp + ya.$$

Mais alors $b = bxp + aby$, et comme p divise ab, il divise nécesairement b. □

THÉORÈME 25. Un anneau intègre principal est factoriel.

Démonstration : Soit A un anneau intègre principal. Montrons que tout élément de A admet une factorisation en éléments irréductibles.

Supposons qu'il existe des éléments qui n'admettent pas de factorisation. On peut alors former l'ensemble non vide S des idéaux (non nuls) de A dont aucun générateur n'a de factorisation. Soit $(x_1) \in S$ et supposons qu'il existe une suite strictement croissante d'idéaux éléments de S :

$$(x_1) \subsetneq (x_2) \subsetneq \cdots .$$

Commençons par démontrer que cette suite ne peut pas être infinie. Si c'était le cas, leur réunion serait un idéal (x) de A (en vertu de la proposition 7). Mais alors x doit appartenir à un des (x_n) ce qui entraînerait que $(x) = (x_n)$ et que la suite est finie.
Ainsi, toute chaîne de S admet un majorant, et d'après le lemme de Zorn, S admet un élément maximal $(x^\star)$ qui contient tous les idéaux éléments de S.

Maintenant, comme $x^\star$ n'admet pas de factorisation en éléments irréductibles, il n'est pas irréductible (sinon il serait sa propre factorisation). Soient alors $a, b \in A$ non inversibles tels que $x^\star = ab$. On obtient $(x^\star) \subsetneq (a)$ et $(x^\star) \subsetneq (b)$ donc par construction de $x^\star$, ni (a) ni (b) n'appartiennent à S. Chacun de ces deux idéaux et alors généré par un élément admettant une factorisation, et à multiplication par un élément inversible près, cela fournit une factorisation de $x^\star$. C'est une contradiction, donc S est vide.

Montrons maintenant l'unicité de la factorisation. Soit $a \in A$ admettant deux factorisations en éléments irréductibles :

$$\prod_{i=1}^{r} p_i = a = \prod_{j=1}^{s} q_j.$$

Alors p_1 divise le produit de droite, et d'après le lemme d'Euclide il divise un des q_i, disons q_1 (quitte à permuter les indices). Il existe alors $u_1 \in A$ inversible tel que $p_1 = u_1 q_1$. Ainsi :

$$u_1 \prod_{i=2}^{r} p_i = \prod_{j=2}^{s} q_j.$$

Par récurrence, on obtient alors l'équivalence des deux décompositions. □

1.2 Définition et propriétés des anneaux noethériens

DÉFINITION 26 *(anneau noethérien).* On dit qu'un anneau A est noethérien si tout idéal de A est engendré par une partie finie.

EXEMPLE 27.
- Un anneau fini est noethérien ;
- un anneau principal est noethérien, car tout idéal est engendré par un élément ;
- l'anneau $\mathbf{Z}$ est noethérien car principal. On pourra en déduire, avec le théorème 40 que $\mathbf{Z}[X]$ est aussi noethérien. C'est donc un exemple d'anneau noethérien non principal. Plus généralement, pour tout $n \in \mathbf{N}$, l'anneau $\mathbf{Z}[X_1, \ldots, X_n]$ est noethérien ;
- les corps sont des anneaux noethériens (les seuls idéaux sont $\{0\}$ et le corps tout entier qui est engendré par 1) ;
- un sous-anneau d'un anneau noethérien n'est pas forcément noethérien (voir l'exemple 29).

PROPOSITION 28. Soit A un anneau. Les trois propriétés suivantes sont équivalentes :
1. A est noethérien ;
2. Toute suite croissante d'idéaux de A est stationnaire ;
3. Tout ensemble non vide d'idéaux de A possède un élément maximal.

Démonstration : $1 \Rightarrow 2$: Supposons A noethérien. Soit $I_1 \subset I_2 \subset \cdots$ une suite croissante d'idéaux de A. Notons $N \overset{\text{def}}{=} \bigcup_{i=0}^{\infty} I_i$ qui est un idéal de A d'après la proposition 8. Donc N est engendré par un nombre fini d'élément $a_1, \ldots, a_n \in A$, où $n \in \mathbf{N}$. Donc $\bigcup_{i=0}^{\infty} I_i = (a_1, \ldots, a_n)$. Pour tout $i \in [\![1, n]\!]$ il existe alors $j_i \in \mathbf{N}$ tel que $a_i \in I_{j_i}$. Prenons $j_0 \overset{\text{def}}{=} \max_{1 \leqslant i \leqslant n} j_i$. Alors $N = (a_1, \ldots, a_n) \subset I_j \subset N$. Ainsi, pour tout $j \geqslant j_0$, $I_j = N$ et la suite est stationnaire.

$2 \Rightarrow 3$: Supposons que toute suite croissante d'idéaux de A est stationnaire. Soit $\mathfrak{I}$ un ensemble non vide d'idéaux de A. Montrons qu'il admet un élément maximal (c.-à-d. qu'il existe $I_0 \in \mathfrak{I}$ et si $I \in \mathfrak{I}$ et $I_0 \subset I$ alors $I = I_0$). Soit $I_0 \in \mathfrak{I} \neq \varnothing$. Si I_0 est un élément maximal de $\mathfrak{I}$, le résultat est vrai. Sinon, il existe $I_1 \in \mathfrak{I}$ tel que $I_0 \subsetneq I_1$. Si $I_0 \subsetneq \cdots \subsetneq I_n$ sont ainsi construits, et si I_n n'est pas un élément maximal, on peut trouver $I_{n+1} \in \mathfrak{I}$ tel que $I_n \subsetneq I_{n+1}$. On construit ainsi une suite strictement croissante d'idéaux de A. La suite doit alors être finie, d'après l'hypothèse. Donc il existe un rang $N \in \mathbf{N}$ tel que I_N est un élément maximal de $\mathfrak{I}$.

$3 \Rightarrow 1$: Supposons que tout ensemble non vide d'idéaux de A possède un élément maximal. Montrons que A est alors noethérien. Soit I un idéal de A. Soit $a_0 \in I$. Si $(a_0) \subsetneq I$ alors il existe $a_1 \in I \setminus (a_0)$. Si $a_0, \ldots, a_n$ sont ainsi construits et si $(a_0, \ldots, a_n) \subsetneq I$ alors il existe $a_{n+1} \in I \setminus (a_0, \ldots, a_n)$. On construit ainsi une suite strictement croissante d'idéaux $((a_0, \ldots, a_n))_{n \in N}$ où $N \subset \mathbf{N}$. Or $\mathfrak{I} \overset{\text{def}}{=} \{(a_0, \ldots, a_n) \mid n \in N\}$ est un ensemble non vide d'idéaux de A. Donc il admet un élément maximal $(a_0, \ldots, a_n)$, où $n \in N$. Alors $N = [\![0, n]\!]$ est fini et $I = (a_0, \ldots, a_n)$. Donc A est noethérien.

□

Exemple 29. L'anneau $\mathbf{Z}[X_0, X_1, \ldots]$ des polynômes en un infinité d'indéterminées n'est pas noethérien. En effet, considérons la suite croissante d'idéaux $(I_i)_{i \in \mathbf{N}}$ telle que pour $i \in \mathbf{N}$, $I_i = (X_0, X_1, \ldots, X_i)$. La suite est strictement croissante : pour tout $i \in \mathbf{N}$, $I_i \subset I_{i+1}$ et $X_{i+1} \notin I_i$. Donc il existe une suite infinie strictement croissante d'idéaux de $\mathbf{Z}[X_0, X_1, \ldots]$. Alors, d'après la proposition 28, $\mathbf{Z}[X_0, X_1, \ldots]$ n'est pas un anneau noethérien.

De plus le corps des fractions de cet anneau est noethérien, étant un corps. Ainsi, $\mathbf{Z}[X_0, X_1 \ldots]$ est un exemple de sous-anneau non noethérien d'un anneau noethérien.

Proposition 30. Soient A et B des anneaux et $\varphi : A \to B$ un morphisme surjectif. Si A est noethérien, alors B l'est aussi.

Démonstration : Supposons A noethérien. Soit I un idéal de B. Alors $\varphi^{-1}(I)$ est un idéal de A. Donc il est engendré par un nombre fini n d'éléments $a_1, \ldots, a_n \in A$. Puisque φ est surjectif, $\varphi(\varphi^{-1}(I)) = I$ donc I est engendré par $\varphi(a_1), \ldots, \varphi(a_n)$. Donc B est bien noethérien. □

Exemple 31. Un anneau noethérien n'est pas forcément factoriel. En effet considérons $\mathbf{Z}[i\sqrt{5}]$. Cet anneau est noethérien comme image de $\mathbf{Z}[X]$ par le morphisme d'anneau d'évaluation en $i\sqrt{5}$. Or il n'est pas factoriel. En effet $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.

$1 + i\sqrt{5}$ est bien irréductible car s'il existe $a, b \in \mathbf{Z}[i\sqrt{5}]$ tq $1 + i\sqrt{5} = ab$, et si on note N le module au carré dans $\mathbf{C}$, alors $N(1 + i\sqrt{5}) = 6 = N(a)N(b)$. Donc ou bien $N(a), N(b) \in \{1, 6\}$ et a ou b est inversible, ou bien $N(a), N(b) \in \{2, 3\}$, ce qui est impossible car $N(a) = \mathfrak{R}(a)^2 + 5\mathfrak{I}(a)^2$ et $\mathfrak{R}(a), \mathfrak{I}(a) \in \mathbf{Z}$. De même pour $1 - i\sqrt{5}$.

Exemple 32. D'autre part, un anneau factoriel n'est pas nécessairement noethérien. Par exemple, l'anneau $\mathbf{C}[X_0, X_1, \ldots]$ est factoriel, pourtant il n'est pas noethérien puisque la suite $((X_0, \ldots, X_n))_{n \in \mathbf{N}}$ est une suite strictement croissante et infinie d'idéaux de $\mathbf{C}[X_0, X_1, \ldots]$.

Proposition 33. Si A est un anneau noethérien intègre, alors pour tout $a \in A$ non nul, non inversible, a est produit fini d'éléments irréductibles.

Démonstration : Considérons l'ensemble $\mathfrak{W}$ des idéaux principaux engendré par chacun des éléments de A non nuls, non inversibles, qui ne s'écrivent pas comme produit fini d'éléments irréductibles. Raisonnons par l'absurde et supposons que $\mathfrak{W}$ est non vide. Donc il admet un élément maximal $I = (a)$. On procède alors comme dans la démonstration du théorème 25 et on aboutit à une absurdité. On conclut que $\mathfrak{W}$ est vide. □

LEMME 34. Un anneau intègre est factoriel si et seulement si toute suite croissante d'idéaux principaux est stationnaire et les éléments irréductibles sont premiers.

PROPOSITION 35. Si A est un anneau noethérien intègre tel que les éléments irréductibles sont premiers, alors A est factoriel.

Démonstration : A est noethérien donc toute suite croissante d'idéaux principaux est bien stationnaire. De plus les éléments irréductibles sont supposés premiers, donc A est bien factoriel, d'après le lemme. □

DÉFINITION 36. Soit A un anneau. On dit qu'un idéal I de A est radiciel s'il vérifie la condition : pour tout $a \in A$, s'il existe $n \in \mathbf{N}$ tel que $a^n \in I$, alors $a \in I$.

DÉFINITION 37. Soient A un anneau et I un idéal de A. Le radical de I est l'ensemble :

$$\sqrt{I} \overset{\text{def}}{=} \{x \in A \mid \exists n \in \mathbf{N}, x^n \in I\}.$$

PROPOSITION 38. Le radical d'un idéal est un idéal radiciel contenant I.

Démonstration : Soient A un anneau, I un idéal de A et $\sqrt{I}$ son radical. Pour $i \in I$, $i \in \sqrt{I}$ en prenant $n = 1$ dans la définition. Donc $I \subset \sqrt{I}$.

De plus $\sqrt{I}$ est bien un idéal de A. En effet $0 \in I \subset \sqrt{I}$. Soient $i, j \in I$. Il existe $n, m \in \mathbf{N}$ tels que $i^n \in I$ et $j^m \in I$. Alors $(i-j)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} i^k j^{n+m-k} (-1)^{n+m-k} \in I$ car pour tout $k \in [\![0, n+m]\!]$, $k \geqslant n$ ou $n+m-k \geqslant m$. Ainsi, $i-j \in \sqrt{I}$. Donc $\sqrt{I}$ est un sous-groupe de $(A, +)$. Enfin, si $a \in A$ et $i \in I$, il existe $n \in \mathbf{N}$ tel que $i^n \in I$ donc $(ai)^n = a^n i^n \in I$. Donc $ai \in \sqrt{I}$, et $\sqrt{I}$ est bien un idéal de A.

Soit $a \in A$ tel qu'il existe $n \in \mathbf{N}$ tel que $a^n \in \sqrt{I}$. Alors il existe $m \in \mathbf{N}$ tel que $(a^n)^m \in I$. Alors $a \in \sqrt{I}$, et $\sqrt{I}$ est bien un idéal radiciel. □

PROPOSITION 39. Soit A un anneau noethérien. Alors tout idéal radiciel de A s'écrit comme intersection finie d'idéaux premiers de A.

Démonstration : Soit $\mathfrak{I}$ l'ensemble des idéaux radiciels qui ne sont pas intersections finies d'idéaux premiers de A. Si $\mathfrak{I}$ n'est pas vide, il admet un élément maximal I. Comme I ne peut pas être premier, on dispose de $a, b \in A \setminus I$ tels que $ab \in I$. Les idéaux $\sqrt{(I, a)}$ et $\sqrt{(I, b)}$ contiennent strictement I donc sont intersections finies d'idéaux premiers, et :

$$\sqrt{(I,a)} \cap \sqrt{(I,b)} = \sqrt{(I,a)(I,b)} = \sqrt{I} = I.$$

C'est absurde, donc $\mathfrak{I}$ est vide. □

THÉORÈME 40 *(de Hilbert).* Soit A un anneau noethérien.
Alors l'anneau $A[X]$ des polynômes à coefficients dans A est noethérien.

Démonstration : Soit $\mathfrak{I}$ un idéal de $A[X]$. Montrons que $\mathfrak{I}$ est de type fini.

Soit, pour tout $i \in \mathbf{N}$:

$$I_i \stackrel{\text{def}}{=} \{a \in A \mid \exists P \in \mathfrak{I}, \exists a_0, \ldots, a_{i-1} \in A, P = aX^i + \cdots + a_1X + a_0\}$$

l'ensemble des coefficients dominants des polynômes de $\mathfrak{I}$ de degré i, uni avec 0. Alors chaque I_i est un idéal de A. En effet, pour tous $a, b \in I_i$, on considère P_a et P_b les polynômes correspondants. Alors ou bien $a = b$ et donc $a - b = 0 \in I_i$, ou bien $P_a - P_b \in \mathfrak{I}$ est de degré i et a pour coefficient dominant $a - b$, qui est donc dans I_i. Enfin, si $a \in A$ et $b \in I_i$, on prend le polynôme correspondant P_b. Alors ou bien $ab = 0 \in I_i$, ou bien aP est de degré i et a pour coefficient dominant ab, donc $ab \in I_i$.

De plus ils forment une suite croissante d'idéaux de A. En effet, soit $i \in \mathbf{N}$. Si $a \in I_i$, il existe $P \in \mathfrak{I}$ de degré i tel que $P = aX^i + \cdots + a_0$. Or, $XP \in \mathfrak{I}$ car $\mathfrak{I}$ est un idéal de $A[X]$, et $XP = aX^{i+1} + \cdots + a_0X$ donc $a \in I_{i+1}$. Mais A est noethérien, donc la suite est stationnaire d'après la proposition 28. Soit $r \in \mathbf{N}$ le rang à partir duquel la suite est constante. Les idéaux $I_0, \ldots, I_r$ sont de type fini, engendrés respectivement par

$$a_{0,1}, \ldots, a_{0,n_0},$$

$$\ldots,$$

$$a_{r,1}, \ldots, a_{r,n_r}.$$

Pour tous $i \in [\![0, r]\!]$ et $j \in [\![1, n_i]\!]$, soit $P_{i,j} \in \mathfrak{I}$ de degré i et de coefficient dominant $a_{i,j}$. Montrons que ces polynômes engendrent $\mathfrak{I}$. Notons alors :

$$\mathfrak{K} \stackrel{\text{def}}{=} (\{P_{i,j},\ i \in [\![0, r]\!],\ j \in [\![1, n_i]\!]\}).$$

Soit $P = b_dX^d + \cdots + b_0 \in \mathfrak{I}$ de degré $d \in \mathbf{N}$. Procédons par récurrence sur d.

Si $d = 0$, $P \in I_0 = (a_{0,1}, \ldots, a_{0,n_0}) \subset \mathfrak{K}$.

Supposons que pour tout $k < d$, tout polynôme de degré k dans $\mathfrak{I}$ est dans $\mathfrak{K}$.

Si $d < r$, il existe $c_1, \ldots, c_{n_d} \in A$ tels que $b_d = \sum_{j=1}^{n_d} c_j a_{d,j}$, et on pose $R \stackrel{\text{def}}{=} \sum_{j=1}^{n_d} c_j P_{d,j}$. Si $d \geqslant r$, puisque $I_d = I_r$, il existe $c_1, \ldots, c_{n_r} \in A$ tels que $b_d = \sum_{j=1}^{n_r} c_j a_{r,j}$, et on pose $R \stackrel{\text{def}}{=} \sum_{j=1}^{n_r} c_j P_{r,j}$.

Dans les deux cas $R \in \mathfrak{K}$, et $Q \stackrel{\text{def}}{=} P - R$ est un polynôme de $\mathfrak{I}$ de degré strictement inférieur à d. Donc par hypothèse de récurrence, $Q \in \mathfrak{K}$. Ainsi $P = Q + R \in \mathfrak{K}$.

On a montré par récurrence que $\mathfrak{I} = \mathfrak{K}$, donc $A[X]$ est un anneau noethérien. □

2 Algèbre différentielle

2.1 Dérivations

Définition 41 *(dérivation).* Soit A un anneau. On appelle dérivation sur A une application $\cdot' : A \to A$ telle que pour tous $a, b \in A$:

$$(a+b)' = a' + b' \quad \text{et} \quad (ab)' = a'b + ab'.$$

Propriétés 42. Pour tous $a, b \in A$ et $n \in \mathbf{N}$:
- on dispose de la formule de Leibniz :
$$(ab)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} a^{(k)} b^{(n-k)};$$
- si n n'est pas nul, $(a^n)' = na^{n-1}a'$;
- $1' = 0$;
- si a est inversible, $(a^{-1})' = -a'a^{-2}$.

Définition 43 *(anneau différentiel).* Un anneau différentiel est la donnée d'un anneau A et d'une dérivation sur A.

Exemple 44.
- La dérivation usuelle sur l'anneau $\mathscr{C}^\infty(\mathbf{R})$ en fait un anneau différentiel ;
- le corps $\mathbf{C}(X)$ des fractions rationnelles à coefficients complexes muni de la dérivation usuelle est un corps différentiel ;
- tout anneau peut être muni de la dérivation triviale qui envoie tout élément sur 0 ;
- ni $\mathbf{Z}$ ni $\mathbf{Q}$ ne peuvent être munis d'une dérivation non triviale. En effet, si l'on munit $\mathbf{Z}$ d'une dérivation $\cdot'$, alors pour tout $n \in \mathbf{N}$, $n' = (1 + \cdots + 1)' = 1' + \cdots + 1' = 0$ et de même si $n \in \mathbf{Z}$. Donc la dérivation est triviale. Si l'on munit $\mathbf{Q}$ d'une dérivation, alors par la proposition suivante elle est triviale sur $\mathbf{Z}$ et pour $a \in \mathbf{Z} \setminus \{0\}$, $(\frac{1}{a})' = (a^{-1})' = -\frac{a'}{a^{-2}} = 0$ car $a' = 0$. Donc la dérivation est triviale.

Théorème 45. Soit A un anneau intègre, muni d'une dérivation. Alors il existe un unique prolongement de cette dérivation sur le corps $\mathbf{K}$ des fractions de A.

Démonstration : Supposons qu'il existe φ une dérivation sur $\mathbf{K}$ qui coïncide avec $\cdot'$ sur A. Alors pour $b \in A \setminus \{0\}$, $\varphi(\frac{1}{b}) = \varphi(b^{-1}) = -\frac{b'}{b^2}$. Donc pour $a, b \in A$, $\varphi(\frac{a}{b}) = \varphi(a)\frac{1}{b} + a\varphi(\frac{1}{b}) = \frac{ba' - ab'}{b^2}$. Cela démontre l'unicité du prolongement.

Pour démontrer son existence, on définit sur $\mathbf{K}$ l'application $\varphi : \frac{a}{b} \mapsto \frac{ba' - ab'}{b^2}$. La définition ne dépend pas du représentant : si $c \in A$, alors

$$\varphi\left(\frac{ac}{bc}\right) = \frac{bc(ac)' - ac(bc)'}{bcbc} = \frac{bca'c + bcac' - acb'c - acbc'}{bcbc} = \frac{ba' - ab'}{b^2} = \varphi\left(\frac{a}{b}\right).$$

De plus cela définit bien une dérivation sur $\mathbf{K}$. En effet, soient $a, b, c, d \in A$. Alors :

$$\varphi\left(\frac{a}{b} + \frac{c}{d}\right) = \varphi\left(\frac{ad + bc}{bd}\right) = \frac{bd(ad+bc)' - (ad+bc)(bd)'}{b^2d^2}$$

$$\begin{aligned} &= \frac{d^2(ba' - ab') + b^2(dc' - cd')}{b^2d^2} \\ &= \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right). \end{aligned}$$

De plus :

$$\varphi\left(\frac{a}{b} \times \frac{c}{d}\right) = \frac{bd(ac)' - ac(bd)'}{b^2d^2} = \frac{bda'c + bdac' - acb'd - acbd'}{b^2d^2}$$
$$= \frac{ba' - ab'}{b^2} \times \frac{c}{d} + \frac{dc' - cd'}{d^2} \times \frac{a}{b}$$
$$= \varphi\left(\frac{a}{b}\right)\frac{c}{d} + \varphi\left(\frac{c}{d}\right)\frac{a}{b}.$$

Donc φ est bien une dérivation sur $\mathbf{K}$ et φ coïncide avec $\cdot'$ sur A. □

EXEMPLE 46. Soient A un anneau différentiel et $a \in A$. On peut alors prolonger la dérivation sur A en *une* dérivation sur $A[X]$ en posant $X' = a$ puis $(X^{(n)})' = nX^{n-1}a$ pour tout $n \in \mathbf{N}^*$. D'après le théorème précédent, on obtient de cette façon *une* structure d'anneau différentiel sur $A(X)$.

DÉFINITION 47 *(polynômes et fractions rationnelles différentielles).* Soit A un anneau différentiel. On munit $A[X_0, X_1, \ldots]$ d'une structure d'anneau différentiel en posant, pour tout $n \in \mathbf{N}$, $X_n' = X_{n+1}$. On note cet anneau $A\{X\}$. Dans $A\{X\}$ on notera $X \overset{\text{def}}{=} X_0$ et pour $n \in \mathbf{N}$, $X^{(n)} \overset{\text{def}}{=} X_n$. Lorsque A est intègre, $A\{X\}$ l'est aussi, et l'on dispose d'un unique prolongement de sa dérivation à son corps des fractions, que l'on note alors $A\langle X\rangle$.

Les anneaux différentiels $A\{X\}$ et $A\langle X\rangle$ sont respectivement appelés l'anneau des polynômes différentiels et l'anneau des fractions rationnelles différentielles à coefficients dans A.

DÉFINITION 48 *(anneau des constantes).* Soit A un anneau différentiel. L'ensemble des éléments de A dont la dérivée est nulle est un sous-anneau de A, appelé l'anneau des constantes de A et noté $C(A)$.

DÉFINITION 49 *(idéal différentiel).* Soient A un anneau et I un idéal de A. On dit que I est un idéal différentiel si pour tout $a \in I$, $a' \in I$.

PROPOSITION 50. Avec les notations de la définition précédente, l'anneau A/I est naturellement muni d'une structure d'anneau différentiel, où la dérivée de la classe $\pi(a)$ d'un élément $a \in A$ est la classe de a'.

Démonstration : Ceci est possible, car si $a, b \in A$ sont tels que $\pi(a) = \pi(b)$, alors $a - b \in I$ donc $a' - b' \in I$, et :

$$\pi(a)' = \pi(a') = \pi(b') = \pi(b)'.$$

□

DÉFINITION 51 *(morphisme).* Soient A et B des anneaux différentiels. On appelle morphisme d'anneaux différentiels un morphisme d'anneaux φ de A vers B qui commute avec la dérivation : pour tout $a \in A$, $\varphi(a') = \varphi(a)'$.

THÉORÈME 52. Soient A et B deux anneaux différentiels et $\psi : A \to B$ un morphisme différentiel. Alors $\operatorname{Ker}\psi$ est un idéal différentiel de A et il existe un isomorphisme différentiel entre $A/\operatorname{Ker}\psi$ et $\operatorname{Im}\psi$.

Démonstration : Si $a \in \operatorname{Ker}\psi$ alors $\psi(a') = \psi(a)' = 0' = 0$, donc $\operatorname{Ker}\psi$ est un idéal différentiel. De plus, l'isomorphisme d'anneaux naturel $\Phi : A/\operatorname{Ker}\psi \cong \operatorname{Im}\psi$ est différentiel. En effet, en notant $\pi : A \twoheadrightarrow A/\operatorname{Ker}\psi$ le morphisme quotient, on a, pour tout $a \in A$:

$$\Phi(\pi(a))' = \psi(a)' = \psi(a') = \Phi(\pi(a')) = \Phi(\pi(a)').$$

Par surjectivité de π, le morphisme Φ est différentiel. □

DÉFINITION-PROPOSITION 53 *(idéal différentiel radiciel engendré).* Pour toute partie S d'un anneau différentiel A, il existe un unique idéal différentiel radiciel de A contenant S et minimal pour l'inclusion. On le note $\{S\}$.

Démonstration : L'intersection d'une famille d'idéaux radiciels est radicielle, et l'intersection d'une famille d'idéaux différentiels est différentielle. Ainsi, $\{S\}$ est l'intersection des idéaux différentiels radiciels qui contiennent S. □

LEMME 54. Soient A un anneau différentiel et I un idéal différentiel *radiciel* de A. Pour tous $a, b \in A$, si $ab \in I$ alors les deux éléments ab' et $a'b$ appartiennent aussi à I.

Démonstration : Par hypothèse, l'élément $(ab)' = a'b + ab'$ appartient à I. Ainsi :

$$(ab)'ab' = aba'b' + (ab')^2 \in I.$$

Donc $(ab')^2 = (ab)'ab' - aba'b' \in I$ et comme I est radiciel, $ab' \in I$. De la même manière, $(a'b)^2 = (ab)'a'b - aba'b' \in I$ et $a'b \in I$. □

LEMME 55. Soient A un anneau différentiel, I un idéal différentiel radiciel de A et $S \subset A$. Alors la partie :

$$T \stackrel{\text{def}}{=} \{x \in A \mid xS \subset I\}$$

est un idéal différentiel radiciel de A, appelé la *saturation* de I par rapport à S.

Démonstration : Commençons par démontrer que T est un idéal. On peut vérifier que $(T, +)$ est bien un sous-groupe de $(A, +)$. De plus, soient $t \in T$ et $a \in A$. Alors $tS \subset I$, donc $taS \subset aI \subset I$, et $ta \in T$. Ensuite, pour tous $t \in T$ et $s \in S$, $ts \in I$ donc d'après le lemme précédent, $t's \in I$, d'où $t' \in T$. Donc T est un idéal différentiel. Enfin, soit $a \in A$ tel que $a^n \in T$ pour un certain $n \in \mathbf{N}^*$. Alors pour tout $s \in S$, $a^n s^n \in I$, et comme I est radiciel, $as \in I$ donc $a \in T$. Dont T est radiciel. □

LEMME 56. Soient A un anneau différentiel, $a \in A$ et S une partie de A. Alors $a\{S\} \subset \{aS\}$.

Démonstration : Soit $T \overset{\text{def}}{=} \{x \in A \mid ax \in \{aS\}\}$. Alors T contient S et, d'après le lemme 55 (avec le singleton a et l'idéal différentiel radiciel $\{aS\}$), c'est un idéal différentiel radiciel. Donc $\{S\} \subset T$, et $a\{S\} \subset \{aS\}$. □

LEMME 57. Soient A un anneau différentiel et S, T deux parties de A. Alors $\{S\}\{T\} \subset \{ST\}$.

Démonstration : Soit $T \overset{\text{def}}{=} \{x \in A \mid x\{T\} \subset \{ST\}\}$. Alors T contient S (d'après le lemme précédent) et est un idéal différentiel radiciel (d'après le lemme 55). Donc $\{S\} \subset T$, et $\{S\}\{T\} \subset \{ST\}$. □

DÉFINITION 58 *(algèbre de Ritt).* On dit qu'un anneau différentiel A est une algèbre de Ritt s'il contient le corps $\mathbf{Q}$. Dans ce cas, $\mathbf{Q}$ est un sous-anneau de $C(A)$, et A est naturellement muni d'une structure de $\mathbf{Q}$-algèbre, via le morphisme d'inclusion $\mathbf{Q} \hookrightarrow A$.

EXEMPLE 59. Les anneaux différentiels suivants ne sont pas des algèbres de Ritt car ils ne contiennent pas $\mathbf{Q}$:
- L'anneau $\mathbf{Z}$ muni de la dérivation triviale ;
- un anneau de polynômes sur un corps fini de cardinal premier $\mathbf{F}_p[X]$ muni de la dérivation usuelle des polynômes.

LEMME 60. Soient A une algèbre de Ritt, I un idéal différentiel de A et $a \in A$ tel que $a^n \in I$ pour un certain $n \in \mathbf{N}^*$. Alors $(a')^{2n-1} \in I$.

Démonstration : Montrons par récurrence que pour tout $k \in [\![1, n]\!]$, $a^{n-k}(a')^{2k-1} \in I$. Le cas $k = n$ démontrera le lemme.

Comme $(a^n)' = na^{n-1}a' \in I$ et que $\mathbf{Q} \subset A$, $\frac{1}{n}(a^n)' = a^{n-1}a' \in I$. Supposons que le résultat est vrai pour un certain $k \in [\![1, n-1]\!]$. Alors la dérivée de $a^{n-k}(a')^{2k-1}$ est un élément de I, c'est-à-dire :

$$(n-k)a^{n-k-1}(a')^{2k-1} + (2k-1)a^{n-k}(a')^{2k-2}a'' \in I.$$

En multipliant par $(a')^2$, $(n-k)a^{n-k-1}(a')^{2k+1} + (2k-1)a^{n-k}(a')^{2k}a'' \in I$. Le membre de droite est dans I par hypothèse, donc $a^{n-k-1}(a')^{2k+1} \in I$. □

LEMME 61. Dans une algèbre de Ritt, le radical d'un idéal différentiel est un idéal différentiel.

Démonstration : D'après le Lemme 38, le radical d'un idéal est bien un idéal. Il découle immédiatement du Lemme 60 que cet idéal est bien différentiel. □

2.2 Théorème de la base (de Ritt-Raudenbush)

Le but de cette sous-section est d'énoncer et démontrer un théorème analogue au théorème de Hilbert (Théorème 40) pour les anneaux différentiels. Le théorème de la base de Hilbert ne s'applique pas directement aux anneaux différentiels. Même si on suppose qu'un anneau différentiel A est noethérien, il n'en va pas de même pour l'anneau différentiel $A\{X\}$. On peut en effet construire une suite strictement croissante d'idéaux de $A\{X\}$: $(X^2), (X^2, X'^2), \ldots, (X^2, \ldots, (X^{(k)})^2), \ldots$ en est un exemple.

THÉORÈME 62 *(de la base de Ritt-Raudenbush).* Soit R une algèbre de Ritt telle que toute suite croissante d'idéaux différentiels radiciels soit stationnaire. Alors il en va de même pour $R\{X\}$.

La démonstration de ce théorème sera donnée après celle du lemme 72.

◇ REMARQUE. L'hypothèse faite sur R est une condition de noethérianité sur ses idéaux différentiels radiciels. Les difficultés de ce théorème viennent justement du fait que les idéaux considérés soient différentiels et radiciels.

On pourra aussi déduire de la démonstration qui suit, le théorème suivant :

THÉORÈME 63. Soit A un anneau tel que toute suite croissante d'idéaux radiciels est stationnaire. Alors il en va de même pour $A[X]$.

DÉFINITION 64. Un idéal différentiel radiciel I d'un anneau différentiel A est dit de type fini s'il existe des générateurs $a_1, \dots, a_n \in A$ tels que $I = \{a_1, \dots, a_n\}$.

LEMME 65. Soient R une algèbre de Ritt, $S \subset R$ et $a \in R$ tels que $\{a, S\}$ soit de type fini. Alors il existe $b_1, \dots, b_n \in S$ tels que $\{a, S\} = \{a, b_1, \dots, b_n\}$.

Démonstration : Notons $J = \{a, S\}$. J est de type fini, donc il existe $c_1, \dots, c_n \in R$ tels que $J = \{c_1, \dots, c_n\}$. Alors les c_i s'écrivent comme combinaisons linéaires de a, d'éléments de S et de leurs dérivées : pour $i \in [\![1, n]\!]$, il existe un nombre fini $n_i \in \mathbf{N}$ d'éléments de S, $s_{i,1}, \dots, s_{i,n_i} \in S$, tels qu'il existe $d_i, d_{i,1}, \dots, d_{i,n_i} \in \mathbf{N}$ et des éléments de R, $(\lambda_{i,k})_{0 \leqslant k \leqslant d_i}, (\mu_{i,1,k})_{0 \leqslant k \leqslant d_{i,1}}, \dots, (\mu_{i,n_i,k})_{0 \leqslant k \leqslant d_{i,n_i}}$ tels que

$$c_i = \sum_{k=0}^{d_i} \lambda_{i,k} a^{(k)} + \sum_{0 \leqslant j \leqslant n_i} \sum_{0 \leqslant k \leqslant d_{i,j}} \mu_{i,j,k} s_{i,j}^{(k)}.$$

Ainsi on peut prendre $(b_i)_{0 \leqslant i \leqslant m} = (s_{i,j})_{\substack{0 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant n_i}}$ qui sont bien des éléments de S. On obtient bien $J = \{a, b_1, \dots, b_m\}$. □

Dans les définitions qui suivent, R est un anneau différentiel et l'on considère l'anneau $R\{X\}$ des polynômes différentiels à coefficients dans R.

DÉFINITION 66 *(ordre d'un polynôme différentiel).* Soit $A \in R\{X\}$. Le plus grand entier naturel $r \in \mathbf{N}$ tel que la dérivée $X^{(r)}$ apparaisse dans A est appelé l'*ordre* de A.

DÉFINITION 67 *(degré d'un polynôme différentiel).* Soient $A \in R\{X\}$ et r son ordre. Le *degré* de A est défini comme le degré de A étant vu comme un polynôme en $X^{(r)}$, c'est-à-dire la plus haute puissance de $X^{(r)}$ qui apparaît dans A.

On dit qu'un polynôme différentiel $B \in R\{X\}$ est *sous* A lorsque l'ordre de B est strictement plus petit que celui de A, ou, si les ordres sont égaux, lorsque le degré de B est plus petit que celui de A. On définit ainsi un préordre sur $R\{X\}$.

Définition 68 *(coefficient dominant).* Pour tout $A \in R\{X\}$ d'ordre r, on dispose de $B, C \in R\{X\}$ et $d \in N$ tels que :

$$A = B \cdot (X^{(r)})^d + C,$$

où $X^{(r)}$ n'apparaît pas dans B et où le degré selon $X^{(r)}$ de C est strictement plus petit que celui de A.

Le polynôme différentiel B est appelé le *coefficient dominant* de A, il est toujours sous A.

Exemple 69. Dans $\mathbf{R}\{X\}$, le polynôme différentiel $4X(X'')^3 + 3X^2X'' + X^3X' - X^4$ est d'ordre 2, de degré 3 et de coefficient dominant $4X$.

Définition 70 *(séparant).* Soient $A \in R\{X\}$ et r son ordre. Le polynôme :

$$S \stackrel{\text{def}}{=} \frac{\partial A}{\partial X^{(r)}}$$

défini comme le polynôme dérivé de A en tant que polynôme en $X^{(r)}$ (c'est-à-dire en voyant les dérivées plus basses de X comme des constantes) est appelé le *séparant* de A. Il est toujours sous A.

Exemple 71. Dans $\mathbf{R}\{X\}$, le polynôme différentiel $4X(X'')^3 + 3X^2X'' + X^3X' - X^4$ a pour séparant le polynôme $12X(X'')^2 + 3X^2$.

Lemme 72. Soient R une algèbre de Ritt, $A \in R\{X\}$, I l'idéal différentiel de $R\{X\}$ engendré par A, B le coefficient dominant de A, S le séparant de A et $F \in R\{X\}$. Alors il existe $m, n \in \mathbf{N}$ et $G \in R\{X\}$ sous A tels que :

$$B^m S^n F \equiv G \pmod{I}.$$

Démonstration : Soient r l'ordre de A et s son degré. On dispose de $T_1 \in R\{X\}$ tel que $A' = SX^{(r+1)} + T_1$, avec l'ordre de T_1 strictement plus petit que $r+1$. En continuant à dériver, on dispose pour tout $k \in \mathbf{N}^*$ de $T_k \in R\{X\}$ d'ordre strictement plus petit que $r+k$ tel que :

$$A^{(k)} = SX^{(r+k)} + T_k.$$

Supposons que F est d'ordre $r+k$ avec $k \in \mathbf{N}^*$. Soit d le degré de F, et soient $W_0, \ldots, W_d \in R\{X\}$ d'ordres $< r+k$ tels que :

$$F = \sum_{i=0}^{d} W_i (X^{(r+k)})^i.$$

Remarquons, que pour tout $i \in \mathbf{N}$, $S^i (X^{(r+k)})^i = (A^{(k)} - T_k)^i \equiv (-T_k)^i \pmod{I}$. Ainsi :

$$S^d F \equiv \sum_{i=0}^{d} W_i S^{d-i} (-T_k)^i \pmod{I}.$$

Le membre de droite est un polynôme différentiel d'ordre strictement plus petit que $r+k$, on peut alors recommencer pour obtenir $n \in \mathbf{N}$ tel que $S^n F \equiv \check{G} \pmod{I}$ avec $\check{G} \in R\{X\}$ de degré $\leqslant r$.

Maintenant, soit $\check{G}$ est d'ordre $< r$ et il est sous A, soit il est d'ordre r. Dans ce dernier cas, supposons qu'il est de degré $s+k$ avec $k \in \mathbf{N}^*$. Soit $W \in R\{X\}$ le coefficient dominant de $\check{G}$ (coefficient devant $(X^{(r)})^{s+k}$). Alors $B\check{G} - W(X^{(r)})^k A$ est d'ordre $\leqslant r$ et, s'il est d'ordre r, de degré $< s+k$. Aussi, le deuxième terme est dans I donc :

$$B\check{G} \equiv B\check{G} - W(X^{(r)})^k A \pmod{I}.$$

On dispose finalement de $m \in \mathbf{N}$ et de $G \in R\{X\}$ sous A tels que $S^m\check{G} \equiv G \pmod{I}$. □

Procédons à la démonstration du Théorème 62.

Démonstration : De la même manière qu'avec la proposition 28, il suffit de montrer que tout idéal différentiel radiciel de $R\{X\}$ est de type fini.

Raisonnons par l'absurde. On suppose qu'il existe un idéal différentiel radiciel qui n'est pas de type fini. Considérons I un tel idéal, maximal pour l'inclusion (c'est possible, d'après le lemme de Zorn).

Montrons que I est un idéal premier. Supposons qu'il existe $a, b \in R$ tels que $ab \in I$ sans que $a \in I$ ni $b \in I$. Alors $\{I, a\}$ et $\{I, b\}$ sont des idéaux différentiels radiciels contenant strictement I, donc ils sont de type fini. Ainsi, par le Lemme 65, il existe $c_1, \ldots, c_n, d_1, \ldots, d_m \in I$ tels que

$$\begin{aligned} \{I, a\} &= \{a, c_1, \ldots, c_n\}, \\ \{I, b\} &= \{b, d_1, \ldots, d_m\}. \end{aligned}$$

Donc, par le Lemme 57 :

$$\begin{aligned} \{I, a\}\{I, b\} &= \{a, c_1, \ldots, c_n\}\{b, d_1, \ldots, d_m\} \\ &\subset \{ab, ad_1, \ldots, ad_n, c_1 b, \ldots, c_1 d_m, \ldots, c_n b, \ldots, c_n d_m\} \\ &\subset I. \end{aligned}$$

Réciproquement, si $z \in I$,

$$z^2 \in \{I, a\}\{I, b\} \subset \{ab, ad_1, \ldots, ad_n, c_1 b, \ldots, c_1 d_m, \ldots, c_n b, \ldots, c_n d_m\},$$

donc $z \in \{ab, ad_1, \ldots, ad_n, c_1 b, \ldots, c_1 d_m, \ldots, c_n b, \ldots, c_n d_m\}$.

Ainsi $I = \{ab, ad_1, \ldots, ad_n, c_1 b, \ldots, c_1 d_m, \ldots, c_n b, \ldots, c_n d_m\}$ et donc I est de type fini, ce qui est contradictoire. Donc I est premier.

$I \cap R$ est un idéal différentiel radiciel de R et donc, par hypothèse, il est de type fini. Notons $J \stackrel{\text{def}}{=} \{I \cap R\}$ l'idéal différentiel radiciel engendré par $I \cap R$ dans $R\{X\}$, J est aussi de type fini. Ainsi, puisqu'on a supposé que I n'était pas de type fini, $J \subsetneq I$.

Soit A un polynôme différentiel de $I \setminus J$ d'ordre r minimal et de degré d minimal pour cet ordre. Alors le coefficient dominant B de A n'appartient pas à I. En effet, si $B \in I$ alors, puisque B est sous A, $B \in J$ par minimalité de l'ordre de A. Et donc $C \in I \setminus J$. Or, C est sous A, ce qui est contradictoire par minimalité de l'ordre de A. Donc on a bien $B \notin I$.

Soit S le séparant de A. Si S était dans I, S serait aussi dans J car S est sous A. Mais alors $A - \frac{1}{d}X^{(r)}S$ serait dans $I \setminus J$, ce qui contredit la minimalité de l'ordre de A. Donc $S \notin I$. (On utilise ici le fait que R est une algèbre de Ritt.)

Puisque I est un idéal premier, $BS \notin I$. Ainsi $\{BS, I\}$ est un idéal différentiel radiciel qui comprend strictement l'idéal I. Donc il est de type fini. Par le Lemme 65, il existe $C_1, \ldots, C_n \in I$ tels que $\{BS, I\} = \{BS, C_1, \ldots, C_n\}$.

Soit $F \in I$. Par le Lemme 72, il existe $m, n \in \mathbf{N}$ et G un polynôme différentiel sous A, tels que $B^m S^n F - G \in \{A\} \subset I$. Donc $G \in I$ et G est sous A, d'où $G \in J$. Ainsi $BSF \in \{J, A\}$ et ce pour tout $F \in I$. Donc $BSI \subset \{J, A\}$.

On en déduit :

$$I^2 \subset I\{BS, I\} = I\{BS, C_1, \ldots, C_n\}$$

$$\begin{aligned} &\subset \{BSI, IC_1, \ldots, IC_n\} \text{ (par le Lemme 57)} \\ &\subset \{J, A, C_1, \ldots, C_n\} \\ &\subset I. \end{aligned}$$

On en déduit que $I = \{J, A, C_1, \ldots, C_n\}$. On aboutit ainsi à une contradiction car on a supposé que I n'était pas de type fini.

On conclut donc que tout idéal différentiel radiciel de $R\{X\}$ est de type fini. □

COROLLAIRE 73. Sous les mêmes hypothèses, on obtient les mêmes conclusions pour tous les $R\{X_1, \ldots, X_n\}$ avec $n \in \mathbf{N}$.

◇ REMARQUE. L'instance la plus importante de ce corollaire est le cas où R est un corps différentiel de caractéristique nulle (R est bien dans ce cas une algèbre de Ritt).

2.3 Applications du théorème de Ritt-Raudenbush

DÉFINITION 74. Soit $\mathbf{K}$ un corps différentiel. Une équation différentielle algébrique (sur $\mathbf{K}$) est une équation de la forme $P(x) = 0$, où P est un polynôme différentiel à coefficients dans $\mathbf{K}$. Une solution est une partie de $\mathbf{K}$ (ou d'une extension différentielle de $\mathbf{K}$) dont les éléments x vérifient $P(x) = 0$.

THÉORÈME 75. Soit $\mathbf{K}$ un corps différentiel de caractéristique nulle. Soit S un ensemble infini d'équations différentielles algébriques sur $\mathbf{K}$ avec un nombre fini d'indéterminées différentielles. Alors il existe un sous-ensemble fini de S avec les mêmes solutions que S.

Démonstration : D'après le Théorème 62, $\{S\}$ est de type fini. Il en découle l'existence d'un nombre fini d'éléments de S qui ont les même solutions sur $\mathbf{K}$ que S. □

On peut énoncer un résultat analogue à la Proposition 39 :

THÉORÈME 76. Soit A un anneau différentiel tel que toute suite d'idéaux différentiels radiciels est stationnaire. Alors tout idéal différentiel radiciel de A est l'intersection d'un nombre fini d'idéaux différentiels premiers.

En particulier, si $\mathbf{K}$ est un corps de caractéristique nulle, le résultat est vrai pour l'anneau différentiel $\mathbf{K}\{X_1, \ldots, X_n\}$.

Démonstration : Raisonnons par l'absurde. Supposons qu'il existe un idéal différentiel radiciel qui n'est pas de type fini. Grâce à l'hypothèse de noethérianité sur les idéaux différentiels radiciels, on peut trouver un idéal différentiel radiciel I maximal pour l'inclusion (pour les idéaux différentiels radiciels qui ne sont pas de type fini). Alors I n'est pas premier. Donc il existe $a, b \in A \setminus I$ tels que $ab \in I$. Or,

$$\begin{aligned} I &\subsetneq \{I, a\} \\ \text{et } I &\subsetneq \{I, b\}. \end{aligned}$$

Donc $\{I, a\}$ et $\{I, b\}$ sont de type fini.

Or d'après le Lemme 57, $\{I, a\}\{I, b\} \subset \{ab, I\} \subset I$. Ainsi, si $c \in \{I, a\} \cap \{I, b\}$, $c^2 \in \{I, a\}\{I, b\} \subset I$. Donc $\{I, a\} \cap \{I, b\} \subset I$.

De plus, $I \subset \{I, a\} \cap \{I, b\}$, donc $I = \{I, a\} \cap \{I, b\}$.

Or, $\{I, a\}$ et $\{I, b\}$ sont de type fini, donc leur intersection I l'est aussi. On aboutit à une contradiction.

Donc tout idéal différentiel radiciel de A est de type fini.

Pour la seconde partie du théorème, on applique le Théorème 62 à $\mathbf{K}\{X_1, \ldots, X_n\}$ pour montrer que cet anneau différentiel vérifie la propriété de noethérianité voulue et la première partie du théorème s'applique. □

On s'intéresse maintenant à l'unicité dans la décomposition en idéaux différentiels premiers.

DÉFINITION 77. On dit que l'écriture d'un idéal I comme intersection d'idéaux est réduite si aucun des idéaux ne peut être omis.

THÉORÈME 78. Soient A un anneau et I un idéal de A. On suppose que I s'écrit de deux façons comme intersection finie d'idéaux premiers :

$$\begin{aligned} I &= P_1 \cap \cdots \cap P_n \\ &= Q_1 \cap \cdots \cap Q_m. \end{aligned}$$

Alors $n = m$ et, quitte à renuméroter les idéaux, $P_i = Q_i$ pour tout $i \in [\![1, n]\!]$.

Démonstration : On peut affirmer $P_1 \cap \cdots \cap P_n \subset Q_1$ et donc $P_1 \cdots P_n \subset Q_1$ car $P_1 \cdots P_n \subset P_1 \cap \cdots \cap P_n$. Ainsi il existe $i \in [\![1, n]\!]$ tel que $P_i \subset Q_1$ car Q_1 est premier. En effet si pour tout $i \in [\![1, n]\!]$ il existait $p_i \in P_i$ tel que $p_i \notin Q_1$, alors en considérant $p_1 \cdots p_n \in Q_1$ on aboutit à une absurdité. On peut supposer que $i = 1$.

De même on montre qu'il existe $j \in [\![1, m]\!]$ tel que $Q_j \subset P_1$. Alors $Q_j \subset Q_1$ et donc $j = 1$, puisque l'intersection est réduite.

Ainsi $P_1 = Q_1$ et on procède de la même manière pour les autres P_i et Q_j. □

Dans toute la suite, on considère un polynôme différentiel A en une indéterminée différentielle X sur un anneau différentiel $\mathcal{A}$. Notons r son ordre et S son séparant. On définit $J \overset{\text{def}}{=} \{B \in \mathcal{A}\{X\} \mid BS \in \{A\}\}$. J est un idéal différentiel radiciel d'après le Lemme 55.

LEMME 79. $\{A\} = \{A, S\} \cap J$.

Démonstration : $\{A\}$ est clairement inclus dans J et dans $\{A, S\}$. Réciproquement, si $C \in J \cap \{A, S\}$, alors $C^2 \in C\{A, S\} \subset \{CA, CS\} \subset \{A\}$. Donc $C \in \{A\}$. □

On suppose dans la suite que $\mathcal{A}$ est un corps différentiel, que l'on notera $\mathbf{K}$, et que l'on supposera de caractéristique 0.

DÉFINITION 80. On dit qu'on polynôme différentiel A est irréductible s'il est irréductible au sens usuel des polynômes en une infinité d'indéterminées, qui sont ici les $X^{(n)}$.

LEMME 81. Supposons que $A \in \mathbf{K}\{X\}$ est irréductible et notons I l'idéal différentiel engendré par A. Soit $G \in I$ d'ordre inférieur ou égal à l'ordre de A. Alors A divise G.

Démonstration : $G \in I$ donc G s'écrit :

$$G = C_0 A + C_1 A' + \cdots + C_k A^{(k)} \tag{1}$$

avec $C_0, \dots, C_k \in \mathbf{K}\{X\}$. Dans le cas où $k = 0$, le résultat est évident. Supposons $k \neq 0$. Soient S le séparant de A et r l'ordre de A. Pour tout $i \in \mathbf{N}^*$, il existe $T_{r+i} \in \mathbf{K}\{X\}$ d'ordre strictement inférieur à $r+i$ tel que $A^{(i)} = X^{(r+i)}S + T_{r+i}$. L'élément $X^{(r+k)}$ n'apparaît pas dans G car l'ordre de G est inférieur ou égal à r. Donc les termes du membre de droite de (1) qui contiennent $X^{(r+k)}$ s'annulent, et on peut *formellement* remplacer tous les $X^{(r+k)}$ par $-T_{r+k}/S$ sans changer l'égalité. Ensuite, on peut multiplier par une certaine puissance S^j de S pour obtenir :

$$S^j G = \check{C}_0 A + \check{C}_1 A' + \cdots + \check{C}_{k-1} A^{(k-1)}$$

avec $\check{C}_0, \dots, \check{C}_k \in \mathbf{K}\{X\}$.
En continuant ainsi, on démontre l'existence de $m \in \mathbf{N}$ tel que A divise $S^m G$. Comme A ne peut pas diviser son séparant et comme il est irréductible, il divise G. □

LEMME 82. Supposons de nouveau que A est irréductible. Alors J est un idéal premier.

Démonstration : Soient $F, G \in \mathbf{K}\{X\}$ tels que $FG \in J$. Montrons que l'un des deux est dans J. Soit I l'idéal différentiel engendré par A. Alors d'après le Lemme 72, il existe $n, m \in \mathbf{N}$ et $F_1, G_1 \in \mathbf{K}\{X\}$ d'ordres inférieurs ou égaux à r tels que

$$\begin{cases} S^m F \equiv F_1 \pmod{I} \\ S^n G \equiv G_1 \pmod{I} \end{cases}.$$

$FG \in J$ donc $SFG \in \{A\}$, par définition de J.

Or $\{A\}$ est un idéal différentiel radiciel contenant A et donc il contient I et son radical. Réciproquement, le radical de I est un idéal différentiel radiciel d'après le Lemme 61, qui contient A, et donc $\{A\}$ par minimalité. Donc $\{A\}$ est le radical de I.

Donc il existe $k \in \mathbf{N}$ tel que $(SFG)^k \in I$. Ainsi $(S^m F)^k (S^n G)^k \in I$ et donc $(F_1 G_1)^k \in I$. Alors, d'après le lemme précédent, A divise $(F_1 G_1)^k$ (l'ordre de $(F_1 G_1)^k$ est bien inférieur ou égal à celui de A, et $(F_1 G_1)^k \in I$). Or A est irréductible et donc divise F_1 ou G_1.

Supposons que A divise F_1. Alors, $S^m F \equiv F_1 \pmod{I}$, et donc $S^m F \in I$. Ainsi $S^m F^m \in I$ et $SF \in \{A\}$. Autrement dit $F \in J$.

Donc J est bien un idéal premier. □

THÉORÈME 83. Soit $\mathbf{K}$ un corps de caractéristique nulle. Soient $A \in \mathbf{K}\{X\}$ irréductible, S son séparant, et $J \overset{\text{def}}{=} \{B \in \mathbf{K}\{X\} \mid BS \in \{A\}\}$.

Alors J est un idéal différentiel premier et si l'écriture de $\{A, S\}$ comme intersection réduite d'idéaux différentiels premiers est $\{A, S\} = P_1 \cap \cdots \cap P_n$ alors celle de $\{A\}$ est de la forme $J \cap P_{i_1} \cap \cdots \cap P_{i_r}$.

Démonstration : D'après le lemme précédent, J est bien un idéal différentiel premier.

D'après le Lemme 79, $\{A\} = \{A, S\} \cap J = J \cap P_1 \cap \cdots \cap P_n$. Il suffit donc de montrer que J n'est pas redondant dans cette écriture. Si J était redondant, alors $J \cap P_1 \cap \cdots \cap P_n = P_1 \cap \cdots \cap P_n$. Donc $P_1 \cap \cdots \cap P_n \subset J$ et donc $\{S, A\} \subset J$. Donc $S \in J$ et $S^2 \in \{A\}$. Alors il existe $k \in \mathbf{N} \setminus \{0\}$ tel que $S^k \in I$, où I est l'idéal différentiel engendré par A, car $\{A\}$ est le radical de I. Ainsi A divise S^k d'après le Lemme 81 et puisque A est irréductible, A divise S, ce qui est absurde. J n'est donc pas redondant dans l'écriture proposée. □

DÉFINITION 84. Avec les notations précédentes, on appelle J la composante de la solution générale (ou composante générale), et les P_i, les composantes des solutions singulières essentielles (ou composantes singulières essentielles).

Exemple 85. Considérons le polynôme différentiel irréductible $A \stackrel{\text{def}}{=} (X')^2 - 4X$. Alors $S = 2X'$ et $\{A, S\}$ est l'idéal engendré par X et ses dérivées, qui est un idéal maximal. De plus $A' = 2X'(X'' - 2) = S(X'' - 2)$.

$X' \in \{A, S\}$. Or $X' \notin \{A\}$ car sinon, d'après le Lemme 81, A diviserait X', ce qui est faux. On en déduit grâce au Lemme 79 que $X' \notin J$.

Or J est premier et $A' \in J$, donc $X'' - 2 \in J$. Donc $K \stackrel{\text{def}}{=} \{(X')^2 - 4X, X'' - 2\} \subset J$.

On peut montrer que K est premier, et $\{A\} = J \cap \{S, A\} \cap K$. Or si on avait $K \subsetneq J$ on pourrait retirer J de l'équation ce qui contredirait le Théorème 83. Ainsi $K = J$.

Trouvons maintenant les solutions de l'équation $(y')^2 - 4y = 0$. Si t est une solution, alors $t'(t'' - 2) = 0$, donc $t' = 0$ ou $t'' = 2$.

Dans le premier cas , $t = 0$.

Dans le second cas, $(\frac{t'}{2})' = 1$. Soit x un élément tel que $x' = 1$. Ainsi, $\frac{t'}{2} = x + c$ et $t = (\frac{t'}{2})^2 = (x + c)^2$, où c est une constante.

Les solutions sont donc les solutions de la composante générale J (les paraboles $y = (x+c)^2$) et la solution singulière $y = 0$.

Bibliographie

[1] Irving Kaplansky, *An Introduction to Differential Algebra*, Hermann, 1957.

[2] Joseph Fels Ritt, *Differential Algebra*, American Mathematical Society, 1950.

[3] Michael Francis Atiyah, Ian Grant MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[4] Serge Lang, *Algebra*, Springer-Verlag, 2002.