N° d'ordre :13 /2011-M/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENNE

FACULTÉ DES MATHÉMATIQUES

MÉMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En : MATHÉMATIQUES

Spécialité : Equations Différentielles dans le Champ Complexe

Par

FERHAT Mohammed Said

THÈME

Sur les solutions algébriques des équations différentielles

Soutenu publiquement, le 02/11/2011, devant le jury composé de :

Mr.	**D. BETINA KAMEL**	Professeur	U.S.T.H.B.	Président.
Mr.	**D. BEHLOUL DJILALI**	Maître de Conférences	U.S.T.H.B.	Directeur de thèse.
Mr.	**D. REZAOUI MED SALEM**	Maître de Conférences	U.S.T.H.B.	Examinateur.
Mr.	**D. LAOUDI AINI**	Maître de Conférences	U.S.T.H.B.	Examinatrice.

Remerciements

Je tiens en premier lieu à exprimer mes plus vifs remerciements à Monsieur **D. *BEHLOUL***, *mon* ***Directeur*** *de thèse pour l'intéressant sujet qu'il m'a proposé. Je lui suis également reconnaissant pour la confiance qu'il m'a accordé.*

L'aventure mathématique de mes années de thèse n'aurait pu débuter sans la confiance qu'a su placer en moi celui qui, aprés avoir ete mon enseignant durant mon année de préparation à l'agrégation, a accepté de devenir mon directeur de thèse. Je remercie **D. *BEHLOUL*** pour sa disponibilité sans faille, sa patience rare, son immense générosité et sa bonne humeur inconditionnelle, son dynamisme et son entrain si communicatifs ont toujours su remotiver mon ardeur au travail. Je dois enfin confesser mon admiration et mon respect pour son inépuisable culture mathématique nourrie d'une profonde passion de la recherche et d'une insatiable curiosite intellectuelle.

Mes remerciments vont aussi au président et autres membres du jury.

Mes pensées vont enfin á ma famille : mes parents, ma femme, mes enfants Adem, Aridj, Imane, mes fréres , mes soeurs, á tous mes amis, sans oublier ceux qui ne sont plus parmi nous mais dont le souvenir demeure toujours aussi vivace dans mon coeur. Merci à chacun d'eux pour m'avoir permis de grandir dans un foyer heureux, insouciant et paisible, pour avoir facilité mes conditions de vie et de travail, pour m'avoir entouré de leur amour et de leur attention, comme un abri contre les orages et les tourments. Rien de tout cela n'aurait été possible sans leur confiance, leur dévotion et leur soutien. Même si ma prose barbare ne leur parle guère, je leur dédie chacune de ces lignes.

Table des matières

Introduction

Les équations différentielles apparaissent dans des domaines ausssi variés que la mécanique du solide, la mécanique des fluides, la biologie, la chimie ...etc.

Récemment en 2011, D.Behloul présente dans (15) une méthode basée sur le polygone de Newton pour déterminer les solutions polynomiales de l'équation de Painlevé généralisée.

Dans (10) Feng et Gao donnent une condition nécessaire et suffisante pour qu'une équation différentielle ordinaire possède une solution générale rationnelle, et présentent un algorithme pour trouver une solution générale rationnelle pour une équation différentielle ordinaire d'ordre 1 à coefficients constants.

Deux résultats importants de Feng et Gao, sont détaillés dans ce mémoire, premièrement on présente une condition nécessaire et suffisante pour qu'une équation différentielle possède une solution générale algébrique. Deuxièment, on décrirera un algorithme pour trouver une solution générale algébrique d'une équation différentielle d'ordre 1 à coefficients constants. On montrera en premier lieu que dans ce cas pour déterminer une solution générale algébrique, il suffit de trouver une solution particulière algébrique. L'algorithme est basé sur la paramétrisation des courbes algébriques planes, l'idée de base est de traiter la variable et ses dérivées comme des variables indépendantes, et l'équation différentielle ordinaire d'ordre 1 définit alors une courbe algébrique plane.

Notre travail est organisé comme suit : le premier chapitre présente des résultats d'algèbre utilisés tout au long de ce mémoire, on y décrit les idéaux polynomiaux, les ensembles caractéristiques. Le second chapitre présente l'algèbre differentiel de Ritt et Kolchin. Dans le chapitre 3, un critère pour qu'une équation différentielle ordinaire a une solution générale algébrique est donné. Dans le chapitre 4, on présentera un algorithme pour calculer une

solution générale algébrique d'une équation différentielle ordinaire d'ordre 1. Un exemple sera donné.

Chapitre 1

Algèbre Commutative

1.1 Extensions algebriques

Définition 1.1.1 *:*

On dit qu'une partie non vide k d'un corps K est un sous corps de K si k est stable pour les lois $+$ et $\times$ et k est un corps pour ces deux lois, on dit aussi que K est une extension de k.

S'il existe un plus petit entier strictement positif n vérifiant $na = 0$ pour tout élément a non nul du corps k, alors la caractéristique de k est n, sinon le caractéristique de k est nulle.

Définition 1.1.2 *:*

Soit k un corps, K une extension de k , θ un élément de K.

S'il existe un polynôme $P \in k[z]$, $P \neq 0$ tel que $P(\theta) = 0$, on dit alors que θ est algébrique sur k, dans le cas contraire θ est dit transcendant sur k.

L'extension K/k est algébrique si tout élément $x \in K$ est algébrique sur k.

Le corps k est algébriquement clos si pour tout polynôme non constant P dans $k[z]$, P a au moins une racine dans k.

Exemple 1.1.1 *:*

1) Les réels e et π sont transcendants sur $\mathbb{Q}$ (théorèmes de Hermite,1873, et de Lindemann, 1882), donc le corps $\mathbb{R}$ est une extension de $\mathbb{Q}$, non algébrique.

2) $\alpha = \sqrt{2} + \sqrt{3}$ est algébrique sur $\mathbb{Q}$, car il existe $P(x)$ dans $\mathbb{Q}[x]$ tel que $P(\alpha) = 0$ ce polynôme est : $P(x) = x^4 - 10x^2 + 1$

3) Le corps $\mathbb{Q}$ n'est pas algébriquement clos, ni $\mathbb{R}$ non-plus.

4) $\mathbb{C}$ est un corps algébriquement clos (Théorème de d'Alembert–Gauß)

Lemme 1.1.1 *:*

Le corps k est algébriquement clos si et seulement si tout polynôme non constant P dans $k[z]$ est le produit de facteurs linéaires (un tel polynôme est dit scindé)

$$P(z) = \mu \prod_{i=1}^{i=n} (z - \lambda_i)^{e_i}$$

où $\mu, \lambda_i \in k$; $n, e_i \in \mathbb{Z}_{>0}$

Corollaire 1.1.1 *:*

Le corps k est algébriquement clos si, et seulement si, tout polynôme irréductible est linéaire.

Définition 1.1.3 *:*

Soit $k \subset K$ une extension algébrique, le degré de K sur k noté $[K : k]$, est la dimension de K comme k-espace vectoriel.

$[K : k] := dim_k K$ et on dit que K/k est finie si $[K : k] < +\infty$ et triviale si $[K : k] = 1$.

Exemple 1.1.2 *:*

1) L'inclusion de corps $\mathbb{R} \subset \mathbb{C}$ est une extension finie : $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2 (la famille $\{1, i\}$ en est une base) et $[C : R] = 2$.

2) Si K est un corps, l'extension $K \subset K(X)$ n'est pas finie. En effet, $K(X)$ contient la famille libre infinie des X^n (pour $n \in N$).

3) Soit $P \in k[X]$ un polynôme irréductible. Le quotient $K := k[X]/(P)$ est un corps, appelé le corps de rupture de P. C'est une extension algébrique finie de k. On a $[K : k] = degP$.

Proposition 1.1.1 *:*

Soient $k \subset K \subset L$ des extensions de corps.

(i) Soient $(\alpha_i)_{i\in I}$ une base de K sur k et $(\beta_j)_{j\in J}$ une base de L sur K.

Alors $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ est une base de L sur k.

(ii) L'extension $k \subset L$ est finie si et seulement si les extensions $k \subset K$ et $K \subset L$ le sont, et on a la relation :

$$[L : k] = [L : K] \times [K : k]$$

Preuve. : Il suffit de prouver (i).

Soit $(\lambda_{ij})_{(i,j)\in I\times J}$ une famille presque nulle d'élements de k alors

$\sum_{i,j}\lambda_{ij}\alpha_i\beta_j = 0 \Longrightarrow \sum_j(\sum \lambda_{ij}\alpha_i)\beta_j = 0$

On a $\lambda_{ij}\alpha_i \in K$ pour tout $(i, j) \in I \times J$. La famille $(\beta_j)_{j\in J}$ etant libre sur K , il vient $\sum_i\lambda_{ij}\alpha_i = 0$, pour tout $j \in J$.

Les $\alpha_i, i \in I$, constituant une base du k-espace vectoriel K , on a alors $\lambda_{ij} = 0$ pour tout $(i, j) \in I \times J$. D'où l'assertion. ■

Corollaire 1.1.2 *:*

Soit $k \subset L$ une extension telle que $[L : k]$ soit premier, alors il n'existe aucun corps K vérifiant $k \subsetneq K \subsetneq L$.

Notation 1.1.1 *:*

Soient $k \subset K$ une extension et S une partie de k. On note $k[S]$ le sous-anneau de K engendré par k et S et $k(S)$ le sous-corps de K engendré par k et S. Il est clair que $k(S)$ est le corps des fractions de $k[S]$. D'autre part, il est immédiat de vérifier que $k[S]$ est l'ensemble des éléments de K qui s'écrivent sous la forme $P(x_1, ..., x_n)$, avec $n \in \mathbb{N}$, $x_1, ..., x_n \in S$ et $P \in k[X_1, ..., X_n]$. De même, $k(S)$ est l'ensemble des éléments $\dfrac{P(x_1, ..., x_n)}{Q(x_1, ..., x_n)}$ de K, avec $n \in \mathbb{N}$, $x_1, ..., x_n \in S$ et $P, Q \in k[X_1, ..., X_n]$ et $Q(x_1, ..., x_n) \neq 0$.

Si $S = \{x_1, ..., x_n\}$, on écrit $k[x_1, ..., x_n]$ pour $k[S]$ et $k(x_1, ..., x_n)$ pour $k(S)$.

L'extension $k \subset K$ est dite de type fini (resp. simple) s'il existe une partie finie S de K (resp. une partie S de K réduite à un élément) telle que $K = k(S)$. Si l'extension est simple, tout élément x de K vérifiant $K = k(x)$ est appelé un élément primitif de l'extension.

Soit K/k une extension et $x \in K$ un élément algébrique. On appelle polynôme minimal de x sur k le générateur unitaire de l'idéal des polynômes dans $k[X]$ annulateurs de x. On notera $Min_k(x)$ le polynôme minimal de x sur k.

Définition 1.1.4 *:*

Un anneau intègre est un anneau non nul sans diviseur de zéro.

Un anneau commutatif intègre est appelé domaine d'intègrité.

Soit k un anneau, une k-algèbre est un anneau A muni d'un homomorphisme d'anneaux : $\varphi : k \longrightarrow A$ (φ n'est pas forcément injectif). Si φ est injectif, on peut identifier k á son image $\varphi(k)$.

Définition 1.1.5 *:*

Soit $k \subset K$ une extension de corps. On dit que K est une clôture algébrique de k si K est algébriquement clos et si tout élément de K est algébrique sur k.

Théorème 1.1.1 *:**(Steinitz, 1910)***

Tout corps admet une clôture algébrique; deux clôtures algébriques sont isomorphes.En fixant une clôture algébrique $\bar{k}$ de k, on peut écrire $P(X) = \mu\prod_{i=1}^{n}(X - a_i)$, avec $n = degP$.

Définition

On appelle corps de décomposition de P ou corps des racines de P le corps $K_P := k[a_1, a_2, ..., a_n]$.On vérifiera que K_P est une extension finie de k et que K_P ne dépend pas du choix de la clôture algébrique $\bar{k}$.

Exemple 1.1.3 *:*

1. Soient $k = \mathbb{Q}$ et $P = X^5 - 2$, alors $K_P = \mathbb{Q}[\sqrt[5]{2}, e^{\frac{2i\pi}{5}}]$.
2. Soient $k = \mathbb{Q}$ et $P = \dfrac{X^p - 1}{X - 1}$ pour p premier, alors $K_P = \mathbb{Q}[e^{\frac{2i\pi}{p}}]$.

Définition 1.1.6 *:*

Soit K/k une extension algébrique finie. Un automorphisme de corps $\sigma : K \longrightarrow K$ qui agit trivialement sur k, c'est-'a-dire $\sigma(x) = x$ pour tout $x \in k$ est appelé un automorphisme de l'extension K/k. L'ensemble des automorphismes de l'extension K/k forme un groupe pour la composition, noté $Aut(K/k)$.

Remarque 1.1.1 *:*

Soit $P \in k[X]$ et soit K_P son corps de décomposition. Si $x \in K_P$ est une racine de P, alors $\sigma(x)$ est aussi une racine de P pour tout automorphisme $\sigma \in Aut(KP/k)$, ceci résulte du calcul suivant : notons $P(X) = \sum_{i=1}^{n} a_i X^i$, avec $a_i \in k$. $P(\sigma(x)) = \sum\limits_{i=1}^{n} a_i \sigma(x)^i = \sigma(\sum\limits_{i=1}^{n} a_i x^i) = \sigma(P(x) = 0$

Définition 1.1.7 *:*

Soient K un anneau commutatif unitaire intègre, A et B deux polynômes de degrés respectifs m et n à coefficients dans K. Les coefficients des polynômes sont notés a_i et b_j, on a donc les égalités :

$$A(z) = \sum_{i=0}^{m} a_i z^i \text{ et } B(z) = \sum_{j=0}^{n} b_j z^j$$

La matrice de Sylvester associée à A et B est la matrice carrée $(n+m) \times (n+m)$ notée $S_{A,B}$, définie ainsi :

$\diamond$ La première ligne est formée des coefficients de A, suivis de 0

$\begin{pmatrix} a_m & a_{m-1} & \ldots & a_1 & a_0 & 0 & \ldots & 0 \end{pmatrix}$

$\diamond$ La seconde ligne s'obtient à partir de la première par permutation circulaire vers la droite

$\diamond$ Les (n-2) lignes suivantes s'obtiennent en répétant la même opération

$\diamond$ La ligne (n+1) est formée des coefficients de B, suivis de 0

$\begin{pmatrix} b_n & b_{n-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \end{pmatrix}$

$\diamond$ les (m-1) lignes suivantes sont formées par des permutations circulaires

$$S_{A,B} = \begin{pmatrix} a_m & a_{m-1} & ... & a_1 & a_0 & 0 & ... & 0 \\ 0 & a_m & a_{m-1} & ... & a_1 & a_0 & ... & . \\ . & . & . & . & . & . & . & 0 \\ . & . & . & a_m & a_{m-1} & ... & a_1 & a_0 \\ b_n & b_{n-1} & ... & b_1 & b_0 & 0 & . & 0 \\ 0 & b_n & b_{n-1} & ... & b_1 & b_0 & . & . \\ . & . & . & . & . & . & . & 0 \\ 0 & . & 0 & b_n & b_{n-1} & ... & b_1 & b_0 \end{pmatrix}$$

Le résultant de A et B par rapport à z noté $Res\,(A, B, z)$ ou $Res_z\,(A, B)$ est le déterminant de la matrice $S_{A,B}$.

On appelle discriminant d'un polynôme A le résultant de A et de A' son polynôme dérivé.

1.2 Calcul des ideaux et comparaison des polynômes :

Etant donné un système d'équations polynomiales, nous cherchons à obtenir des renseignements sur ses solutions.

Pour ce faire, nous calculons une famille d'ensembles particulières (appelés ensembles caractéristiques) dont la réunion des solution coincide avec les solutions du système initial.

Nous donnons d'abord la définition suivante .

Définition 1.2.1 *:*

Un idéal d'un anneau A est un sous-groupe additif I de A, tel que pour tout $a \in A$ et tout $x \in I$, on a : $ax \in I$.

C'est à dire que la partie I vérifie :

- $0 \in I$
- Si $a \in I$ et $b \in I$, $a + b \in I$
- Si $a \in A$ et $x \in I$, $ax \in I$.

Proposition 1.2.1 *:*

L'intersection d'une famille non vide d'idéaux est un idéal.

Corollaire 1.2.1 *:*

Soit S une partie d'un anneau A, alors il existe un plus petit idéal de A contenant S, noté $\langle S \rangle$.

On l'appelle l'idéal engendré par S, et on a pour tout idéal I de A contenant S :

$S \subset \langle S \rangle \subset I$ et $\langle S \rangle = \{\sum a_s x_s \ / \ a_s \in A, x_s \in S\}$

Un idéal principal est un idéal engendré par un élément a, c'est l'idéal : aA

Un idéal de génération fini est un idéal engendré par une partie finie $\{a_1, ..., a_n\}$, c'est l'idéal : $a_1 A + ...a_n A$.

Exemple 1.2.1 *:*

(1) Dans $\mathbb{Z}$ tous les sous-groupes additifs sont de la forme $n\mathbb{Z}$.

(2) Si A est un corps, les seuls idéaux de A sont (0) et A.

Définition 1.2.2 *:*

Soient I et J deux ideaux de l'anneau A

a) L'idéal engendré par $I \cup J$ est :

$$I + J = \{i + j / (i, j) \in I \times J\}$$

On appelle cet idéal la somme de I et J.

b) L'idéal engendré par l'ensemble des produits $ij, (i, j) \in I \times J$ est :

$$IJ = \left\{ \sum_k i_k j_k \ , \forall k \ \ (i_k, j_k) \in I \times J \right\}$$

cet idéal est appelé le produit de I et J.

c) Le radical de I est l'ensemble des éléments a de A pour lesquels il existe $n \in \mathbb{N}^*$ vérifiant $a^n \in I$,

C'est un idéal de A qui contient I, et on le note note $\sqrt{I}$

$$\sqrt{I} = \{a \in A; \text{il existe } n > 1, a^n \in I\}$$

Proposition 1.2.2 *:*

Soit I un idéal de l'anneau A et soit S une partie de A. On définit le conducteur de S dans I par la formule

$$J = (I : S) = \{a \in A \text{ ; pour tout } s \in S \text{ , } as \in I\}$$

l'ensemble J est un idéal de A.

Preuve. : Il est clair que la somme de deux éléments de J est contenu dans J

En effet si $a, b \in J$, alors pour tout $s \in S$, $as \in I$ et $bs \in I$

et comme $(a+b)\, s = as + bs$; et I est un idéal, alors $(a+b)\, s \in I$

donc $a + b \in J$.

De même pour le produit d'un élément de A par un élément de J, le produit est encore dans J.

En effet si $a \in J$ et $c \in A$, alors pour tout $s \in S$, $as \in I$

et comme $(ca)\, s = c\,(as)$ et I est un idéal, alors $(ca)\, s \in I$

donc $ca \in J$. ■

Définition 1.2.3 *:*

Soit A un anneau et soit I un idéal de A.

On dit que I est un idéal premier s'il vérifie :

$$I \neq A \text{ et } \forall a, \forall b \text{ ; } ab \in I \Rightarrow a \in I \text{ ou } b \in I.$$

On dit que I est maximal s'il est distinct de A et si les seuls idéaux de A qui contiennent I sont I et A.

Exemple 1.2.2 *:*

Dans un anneau commutatif, tout idéal maximal est premier.

Dans $\mathbb{Z}$ l'idéal nul (0) est premier, mais n'est pas maximal. Les autres idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$,avec p premier. Ils sont maximaux.

Théorème 1.2.1 *:*

(1) Un idéal I d'un anneau A est premier si et seulement si l'anneau quotient A/I est intègre.

(2) Un idéal I d'un anneau A est maximal si et seulement si A/I est un corps.

Preuve. : (1) Supposons que l'anneau quotient A/I est intègre.

Par définition $A/I \neq \{0\}$ c'est a dire que $I \neq A$,et ensuite que si un produit xy d'éléments de A/I est nul, alors x ou y est nul. Ecrivons $x = cl(a)$ et $y = cl(b)$ avec a et b dans A.

Comme: $xy = cl(a)cl(b) = cl(ab)$, alors $xy = 0$ équivaut à $ab \in I$,

et $x = 0$ ou $y = 0$ équivaut à $a \in I$ ou $b \in I$.

(2) Supposons que l'anneau quotient A/I est un corps. Comme l'anneau nul n'est pas un corps, $A/I \neq \{0\}$ c'est a dire que $I \neq A$, soit d'autre part un ideal J de A contenant I.

Si $J \neq I$, il existe ainsi $a \in J \backslash I$, sa classe $cl\,(a) \in A/I$ et donc non nul, donc inversible puisque A/I est un corps. Il existe donc $b \in A$ tel que $cl\,(a)\,cl\,(b) = 1$.On a donc $ab - 1 \in I$, par suite $ab - 1 \in J$, et comme $a \in J$, $1 = ab - (ab - 1) \in J$. Par suite $J = A$, d'où I est un l'idéal maximal.

Réciproquement, si I est maximal alors $A/I \neq \{0\}$, puisque $I \neq A$, si $x \in A/I$ est non nul, il existe $a \in A$ tel que $x = cl\,(a)$ et l'on a $a \notin I$. L'ideal $J = I + (a)$ contient I; comme il contient a, alors $J \neq I$. Par hypothèse, on a $J = I + (a) = A$, ce qui signifie qu'il existe $u \in I$ et $b \in A$ tels que $1 = u + ab$, alors dans l'anneau A/I, on a $1 = cl\,(1) = cl\,(u + ab) = cl\,(a)\,.cl\,(b) = x.cl\,(b)$, ce qui prouve que x est inversible dans A/I.

■

Définition 1.2.4 *:*

Un idéal B d'un anneau A est parfait si et seulement si:

$$a^p \in B \implies a \in B \quad (p \text{ entier} > 0)$$

Il est facile de vérifier que tout idéal premier est parfait.

L'intersection de tous les idéaux parfaits contenants B est un ideal parfait noté $\{B\}$. Et on a les formules:

$$\{BC\} = \{B\} \cap \{C\}$$

$$\{B \cup CD\} = \{B \cup C\} \cap \{B \cup D\} \tag{1.2.1}$$

Proposition 1.2.3 *:*

Pour tout idéal I de l'anneau A, il existe une décomposition en idéaux parfaits indécomposables.

$$I = I_1 \cap I_2 \cap ... \cap I_p$$

Tout idéal premier est irréductible (et à fortiori indécomposable).

Réciproquement : Tout idéal parfait indécomposable est premier.

En effet si I n'est pas premier, il existe $a \notin I$ et $b \notin I$ tel que $ab \in I$ et on a d'aprés la relation (1.2.1) :

$$I = \{I \cup ab\} = \{I \cup a\} \cap \{I \cup b\}$$

donc I n'est pas indécomposable .

On a dans ce cas, une décomposition en idéaux premiers, elle est unique si l'on supprime les diviseurs premiers surabondants, les diviseurs restants sont appelés diviseurs premiers essentiels.

Définition 1.2.5 *:*

Soit l'anneau $A = k[X_1, ...X_n]$ et K une extension de k et S est une partie de A

On dit que $t = (t_1, ..., t_n) \in K^n$ est un zéro de P si $P(t_1, ..., t_n) = 0$ i.e. $P(t) = 0$.

On dit que $t = (t_1, ..., t_n) \in K^n$ est un zéro de S dans K^n si t est un zéro commun à tous les polynômes P de S.

On dit que $t = (t_1, ..., t_n) \in K^n$ est un zéro générique de S si pour tout polynôme P de A :

$$P(t) = 0 \implies P \in S$$

On note $V_K(S)$ l'ensemble des zéros de S dans K^n et on dit que c'est la variété des zéros de S dans K^n.

Soit M une partie de K^n, l'ensemble des $P \in A$ tel que $P(t) = 0$ pour tout $t \in M$ est un idéal de A, noté $i(M)$.

Il est clair que $\sqrt{i(M)} = i(M)$.

En outre, si I est un idéal de A, on a : $I \subset i(V_K(I))$ donc $\sqrt{I} \subset i(V_K(I))$

Proposition 1.2.4 *:*

Tout idéal premier a un zéro générique.

Définition 1.2.6 *:*

Soit K un anneau commutatif et n un entier naturel > 1. Nous considèrons l'ensemble $\mathbb{N}^n$ des n-uplets d'entiers positifs ou nuls $v = (v_1, ..., v_n)$.

Un polynôme à n indéterminées à coefficients dans K est une famille $(a_v)_{v \in \mathbb{N}^n}$ dont tous les termes sont nuls, à l'exception d'un nombre fini.

L'ensemble de tous ces polynômes est un anneau commutatif noté $K[X_1, X_2, ..., X_n]$, muni des lois suivantes :

$$(a_v) + (b_v) = (a_v + b_v)$$

$$(a_u).(b_v) = (c_w) = \sum_{u+v=w} a_u b_v$$

Avec ces notations le polynôme $A = (a_v)_{v \in \mathbb{N}^n}$ s'écrit :

$$A = \sum_{v \in \mathbb{N}^n} a_v X_1^{v_1} X_2^{v_2} ... X_n^{v_n} = \sum_{v_1,...,v_n \in \mathbb{N}} a_{v_1,...,v_n} X_1^{v_1} X_2^{v_2} ... X_n^{v_n}$$

Le degré de $A \in K[X_1, X_2, ..., X_n]$ par rapport à X_k est le degré de A, considéré comme un polynôme en X_k à coefficients dans $K[X_1, ..., X_{k-1}, X_{k+1}, ..., X_n]$ et on le note $deg_k(A)$, il est aussi la plus haute puissance avec laquelle intervient X_k dans un monôme $a_v X_1^{v_1} X_2^{v_2} ... X_n^{v_n}$ de A, si $A \neq 0$. (Si $A = 0$, on rappelle que $deg_k(A) = -\infty$), on a les formules :

$$deg_k(A + B) \leq \sup(deg_k(A), deg_k(B))$$

$$deg_k(AB) \leq deg_k(A) + deg_k B \tag{1.2.2}$$

Le degré total $deg(A)$ de A est : $-\infty$ si $A = 0$, et $\underset{a_v \neq 0}{sup}(v_1 + ... + v_n)$ si $A \neq 0$, on a les formules :

$$deg(A+B) \leq \sup(deg(A) + deg(B))$$

$$deg_k(A+B) \leq deg(A) + degB \tag{1.2.3}$$

Si K est intègre, on a l'égalité dans (1.2.2) et (1.2.3)

Définition 1.2.7 *:*

Soit A un polynôme dans $K[X_1, X_2, ..., X_n]$.

On appelle classe de A, le plus grand indice k tel que X_k apparaisse dans A, on le note $cls(A)$. Si $A \in K$, alors $cls(A) = 0$.

On appelle classe degré de A, le degré de A par rapport à X_k, on le note $cdeg(A)$.

Avec ces notations un polynôme A de classe k et $cdeg(A) = d$ peut s'écrire :

$$A = I_d(X_1, X_2, ..., X_{k-1}) X_k^d + I_d(X_1, X_2, ..., X_{k-1}) X_k^{d-1} + ... + I_0(X_1, X_2, ..., X_{k-1}) \tag{1.2.4}$$

où $I_t(X_1, X_2, ..., X_{k-1}) \in K[X_1, X_2, ..., X_{k-1}]$ pour $t = 0, ..., d$

Le polynôme initial de A noté $In(A)$ est défini comme étant le polynôme $I_d(X_1, X_2, ..., X_{k-1})$ dans (1.2.4)

Le séparent de A est le polynôme: $S = \dfrac{\partial A}{\partial X_k}$

On appelle ordre de A relativement à X_k , le plus grand indice j tel que X_{kj} apparaisse effectivement dans A.

On dit que A_1 est de rang inférieur à A_2 relativement à X_k, soit si l'ordre de A_1 est inférieur à celui de A_2, soit s'ils ont le même ordre j pour X_k et $deg_k(A_1) < deg_k(A_2)$, et on note : $A_1 < A_2/X_k$.

On dit que A_1 est inférieur à A_2 , soit si $cls(A_1) < cls(A_2)$, soit si $cls(A_1) = cls(A_2) = k$, et si $A_1 < A_2/X_k$. et on note : $A_1 < A_2$.

Si $A_1 \not< A_2$, ni $A_1 \not< A_2$, alors $A_1 < A_2$ sont dits de même rang et on note : $A_1 \backsimeq A_2$.

On dit que A_2 est réduit pour A_1 si A_1 est de classe $k > 0$ et $A_2 < A_1/X_k$.

Lemme 1.2.1 *:*

Soit A un polynôme de $K[X_1, ..., X_n]$ avec $cls(A) = k > 0$, S et I étant le séparent et l'inital de A, alors pour tout polynôme B de $K[X_1, ..., X_n]$ il existe deux polynômes Q et R et deux entiers non négatifs s et t tels que R est réduit pour A et :

$$S^s.I^t.B = A.Q + R \tag{1.2.5}$$

Si de plus s et t sont les plus petits entiers possible qui vérifient (1.2.5) , alors Q et R sont uniques, et dans ce cas le polynôme R est appellé le pseudo-reste de B par rapport à A et on le note $prem(A, B)$.

Définition 1.2.8 *:*

Une suite de polynômes $A_1, ..., A_r$ pris dans cet ordre, constitue une chaîne, soit si $r = 1$ et $A_1 \neq 0$, soit si les classes des A_i sont positives et croissantes, et chacun d'eux étant réduit pour tous ses prédécesseurs.

Une chaîne a au plus n termes.

Une chaîne $\Phi_1 = A_1, A_2, ..., A_r$ est dite inférieure à $\Phi_2 = B_1, B_2, ..., B_s$, soit si $A_i = B_i$ pour tout $i \leq q$ et $A_{q+1} < B_{q+1}$, soit si $r > s$ et $A_i \approx B_i$ pour tout $i \leq s$.

Remarque 1.2.1

Dans un système T de polynômes, il existe un polynôme de rang minimum; il existe une chaîne de rang minimum. Une telle chaîne est appelée chaîne caractéristique de T.

Un système T_1 sera dit inférieur à un système T_2 si toute chaîne caractéristique de T_1 est inférieure à toute chaîne caractéristique de T_2.

Un polynôme B est dit réduit pour la chaîne $\Phi = A_1, A_2, ..., A_r$ s'il est réduit pour tous les A_i de Φ

Théorème 1.2.2 *:*

Soit $\Phi = A_1, A_2, ..., A_r$ une chaîne du système T.

Φ est une chaîne caractéristique du système T si et seulement si aucun polynôme non nul de T n'est réduit pour la chaîne Φ.

Preuve. :(1) Supposons $F \in T$ et $F \neq 0$, F est réduit pour $\Phi = A_1, A_2, ..., A_r$.

Supposons que la classe de F est superieure à celle de A_j et non à celle de A_{j+1}

le système $A_1, A_2, ..., A_r$ est une chaîne inférieure à $\Phi = A_1, A_2, ..., A_r$, donc Φ n'est pas caractéristique.

(2) Supposons Φ non caractéristique du système T et $\Phi > \Psi = B_1, B_2, ..., B_s$

▶ Si $A_i \backsimeq B_i$ pour tout $i \leq q$ et $A_{q+1} > B_{q+1}$, on prendra $F = B_{q+1}$.

▶ Soit si $r < s$ et $A_i \backsimeq B_i$ pour tout $i \leq r$, on prendra $F = B_{r+1}$.

Donc F est réduit pour la chaîne Φ. ■

Chapitre 2

Algèbre différentielle

2.1 Structures differentielles :

Définition 2.1.1 *:*

Soient B un anneau et A un sous-anneau de B, une dérivation de A dans B est une application $D:\ A \longrightarrow B$ vérifiant pour tout $x, y \in A$,

$$D(x+y) = D(x) + D(y) \quad , \quad D(xy) = xD(y) + yD(x)$$

On note $Der(A, B)$ l'ensemble des dérivations de A dans B.

Lemme 2.1.1 *:*

Soit D une dérivation de $Der(A, B)$, alors :

1- $D(1) = 0$.

2- Si $x \in A$ et $n \in \mathbb{N}^*$ alors $D(x^n) = nx^{n-1}D(x)$.

3- Si x et inversible dans A alors $D(x^{-1}) = -x^{-2}D(x)$.

4- Soient $x, y \in A$ et $n \in \mathbb{N}$, alors

$$D^n(x.y) = \sum_{i=0}^{n} C_n^i D^i(x) D^{n-i}(y)$$

Preuve. : (1) De $1 = 1.1$, on a $D(1) = 1.D(1) + D(1) = 2D(1)$. D'où $D(1) = 0$.

(2) Écrivant $D\left(x^{n+1}\right) = xD\left(x^n\right) + x^n D\left(x\right)$, l'assertion s'obtient par récurrence.

(3) Cela résulte de $1 = xx^{-1}$ et de (1)

(4) C'est immédiat par récurrence sur n. ■

Proposition 2.1.1 *:*

Soient K un corps et A un sous-anneau de K et k le corps des fractions de A, tout élément de $Der\left(A, K\right)$ se prolonge de manière unique à un élément de $Der\left(k, K\right)$.

Preuve. : Supposons que D se prolonge en Δ . Soient $a \in A, b \in A^*$ et $x = \dfrac{a}{b}$. D'après le lemme précédent, on a nécessairement:

$$\Delta\left(x\right) = \frac{bD\left(a\right) - aD\left(b\right)}{b^2}$$

Pour obtenir le résultat, il faut que cette expression ne dépend pas du représentant a/b de x et qu'elle définit une dérivation de k dans K.

Soit $c \in A^*$, il vient $\dfrac{\left(bc\right)D\left(ac\right) - \left(ac\right)D\left(bc\right)}{\left(bc\right)^2} = \dfrac{bD\left(a\right) - aD\left(b\right)}{b^2}$ d'où le premier point.

Soient $x = a/b$ et $y = c/d$, alors :

$$\Delta\left(x+y\right) = \Delta\left(x\right) + \Delta\left(y\right) \quad , \quad \Delta\left(xy\right) = x\Delta\left(y\right) + y\Delta\left(x\right)$$

d'où le le résultat. ■

Exemple 2.1.1 *:*

La dérivation usuelle de $k\left[X\right]$ se prolonge de manière unique en une dérivation de $k\left(X\right)$ dans lui même. On note encore $F \longrightarrow F\prime$ ce prolongement; et on dit que c'est la dérivation usuelle de $k\left(X\right)$.

Lemme 2.1.2 *:*

Soit k un corps, on munit $A = k[T]$ et $K = k(T)$ de leur dérivation usuelle et on pose

$$A_0 = \left\{P \in k[T]; P' = 0\right\} \quad , \quad K_0 = \left\{F \in k\left(T\right)[; F' = 0\right\}$$

(1) Si k est de caractéristique 0, $A_0 = K_0 = k$.

(2) Si k est de caractéristique $p > 0$, $A_0 = k[T^p]$ et $K_0 = k(T^p)$.

Preuve. : Si $P = \sum_{n=0}^{N} a_n T^{\,n}$, $P' = \sum_{n=0}^{N} n a_n T^{\,n-1}$.

Supposons $P' = 0$, c'est-à-dire : $na_n = 0$ pour tout n.

Si k est de caractéristique nulle, cela entraîne $P = a_0$.

Si k est de caractéristique p, cela implique seulement que $a_n = 0$ si n n'est pas multiple de p, d'où $P \in k[T^p]$. L'autre inclusion est évidente.

Passons aux fractions rationnelles et soit R une fraction rationnelle telle que $R' = 0$. Ecrivons $R = A/B$ où A et B sont deux polynômes, B étant non nul et de degré minimal. On a alors $BR = A$, d'où, en dérivant , $B'R = A'$, le degré de B' est strictement inférieur à celui de B, donc l'hypothèse de minimalité entraîne que $B' = 0$, d'où $A' = B'R = 0$.

Si k est de caractéristique 0, A et B sont des polynômes constants.

Si k est de caractéristique p, A et B sont des polynômes en $T^{\,p}$, donc $R \in k(T^p)$.

Réciproquement, une telle fraction rationnelle est de dérivée nulle. ■

Définition 2.1.2

On appelle anneau différentiel un couple (A, D), où A est un anneau et D un élément de $Der\,(A, A)$. Quand l'anneau est un corps, on parle plutôt de corps différentiel.

Un élément d'un anneau différentiel est dit constant si sa dérivée est nulle.

Exemple 2.1.2 *:*

On définit un polynôme différentiel à une indéterminée y à coefficients dans le corps K comme étant le polynôme en $y, y_1, ..., y_n$ à coefficients dans K, les y_i sont les derivées de l'indeterminée différentielle y. L'ensemble des polynômes différentiels à coefficients dans le corps K est un anneau différentiel noté $K\{y\}$.

Notation 2.1.1 *:*

Soit $A\,(y)$ un polynôme différentiel dans $K\{y\}$.

L'ordre de $A\,(y)$ est la plus grande derivée de y dans $A\,(y)$, noté $ord\,(A\,(y))$.

En prenant $ord\,(A\,(y)) = q$, on pourra regarder $A\,(y)$ comme un polynôme algébrique en $y, y_1, ..., y_n$ à coefficients dans K et l'initial I, séparent S, $deg\,(A\,(y))$ et $tdeg\,(A\,(y))$ sont définis comme dans le cas algébrique, on a :

$$A = I.y_q^d + B$$

Avec $ord\,(I\,(y)) < q$, et $B\,(y) < A\,(y)$.

La $h^{éme}$ dérivée de A est notée par $A^{(h)}$ et on a :

$$A^{(h)} = S.y_{q+h} + C \tag{2.1.1}$$

Avec $ord\,(C\,(y)) < q + h$, et $S\,(y) < A\,(y)$.

La définition de zéro générique est toujours la même que dans le cas algébrique.

Pour un polynôme différentiel $A\,(y)$ d'ordre q, un polynôme $B\,(y)$ est dit réduit par rapport à $A\,(y)$ si $ord\,(B) < q$ ou $ord\,(B) = q$ et $deg_q\,(B) < deg_q\,(A)$

Pour deux polynômes differentiels $A\,(y)$ et $B\,(y)$, soit $R = prem\,(A, B)$ le pseudo-reste de A par rapport à B, on a la formule suivante :

$$J.A = \sum M_i\,(y)\,.B^i\,(y) + R\,(y) \tag{2.1.2}$$

où $J\,(y)$ est un produit de certaines puissances de l'initiale et du séparent de $B\,(y)$ et $B^i\,(y)$ est la $i^{éme}$ dérivée de $B\,(y)$ et $M_i\,(y)$ sont des polynômes differentiels.

Le polynôme $A\,(y)$ est irréductible, si $A\,(y)$ est algébriquement irréductible, c'est à dire qu'il ne peut s'écrire comme produit de deux polynômes differentiels de classes positives.

Proposition 2.1.2 *:*

Soit (A, D) un anneau différentiel, l'ensemble des $a \in A$ tels que $D(a) = 0$ est un sous-anneau de A. Si (K, D) est un corps différentiel, l'ensemble des $a \in K$ tels que $D(a) = 0$ est un sous-corps de K ; on l'appelle le corps des constantes.

Preuve. : Si a et b vérifient $D(a) = D(b) = 0$, on a $D(a + b) = D(a) + D(b) = 0$ et $D(ab) = aD(b) + bD(a) = 0$.

On a vu que $D(1) = 0$ ainsi, l'ensemble des $a \in A$ tels que $D(a) = 0$ est un sous-anneau de A.

Si $a \in A$ est inversible et vérifie $D(a) = 0$, le lemme précédent montre que $D(1/a) = 0$, donc $1/a$ est constant, d'où l'ensemble des éléments $x \in K$ tels que $D(x) = 0$ est un sous-corps de K. ■

Définition 2.1.3 *:*

Soient (A, D) et (B, Δ) deux anneaux differentiels.

(1) On appelle idéal différentiel de A tout idéal I de A tel que $D(I) \subset I$.

$$a \in I \implies a\prime \in I$$

Les définitions d'idéaux premiers et d'idéaux parfaits sont les mêmes que dans le cas algébrique.

(2) Un homomorphisme de corps différentiels $u : (A, D) \longrightarrow (B, \Delta)$ est un homomorphisme au sens algébrique, qui commute avec les dérivations, i/e. :

$$\begin{aligned} u(0_A) &= u(0_B) \\ u(1_A) &= u(1_B) \\ u(a + a') &= u(a) + u(a') \\ u(aa') &= u(a).u(a') \\ u(D(a)) &= \Delta(u(a)) \end{aligned}$$

On peut de même définir un isomorphisme et un automorphisme de corps differentiels .

Lemme 2.1.3 *:*

Soit $u : (A, D) \longrightarrow (B, \Delta)$ un homomorphisme d'anneaux différentiels, alors $Ker(u)$ est un idéal différentiel de A.

Preuve. : Soient $a, b \in Ker(u)$, alors $u(a) = 0$, $u(b) = 0$, comme $u(a+b) = u(a)+u(b)$ donc $u(a + b) = 0$, d'où $a + b \in Ker(u)$.

Soient $a \in Ker(u)$, $c \in A$; alors $u(ca) = cu(a) = 0$ donc $ca \in Ker(u)$.

D'autre part si $a \in Ker(u)$, on a $u(D(a)) = \Delta(u(a)) = \Delta(0) = 0$

d'où $D(a) \in Ker(u)$, donc $Ker(u)$ est un idéal différentiel de A. ■

Théorème 2.1.1 *:*

Si I est un idéal parfait de (A, D)et si $ab \in I$, alors $D(a)\, b \in I$.

Preuve. L'idéal I contient ab, donc il contient $D(ab)$ car I est différentiel.
I contient donc $D(a)\, b.D(ab)$ car I est un idéal.

$$\begin{aligned} D(a)\, b.D(ab) &= D(a)\, b.\left(aD(b) + bD(a)\right) \\ &= abD(a)\, D(b) + \left(D(a)\, b\right)^2 \end{aligned}$$

Comme $abD(a)\, D(b) \in I$ donc $\left(D(a)\, b\right)^2 \in I$, d'où I contient $D(a)\, b$ car I est parfait .

■

Corollaire 2.1.1 *:*

Si I est un idéal parfait de (A, D) , et si $ab \in I$, alors chaque $[D(a)]^{(i)}\, [D(b)]^{(j)} \in I$.

2.2 Extensions de Piccard-Vessiot :

De la même façon qu'on a construit le corps de décomposition d'un polynôme qui est une extension algébrique minimale contenant les racines de ce polynôme, nous allons construire une extension minimale d'un corps différentiel dans laquelle une équation différentielle linéaire d'ordre n admet n solutions linéairement indépendantes.

Les corps considérés sont supposés de caractéristique nulle. On désigne par (k, D) un corps différentiel et par k_0 son corps des constantes.

Définition 2.2.1 *:*

Soient (k, D) et (K, Δ) deux corps différentiels, avec K une extension algébrique de k.
On dit que K est une extensoin différentielle de k, si pour tout $a \in k$

$$\Delta(a) = D(a)$$

Afin de simplifier les notations, si (K, Δ) est une extensoin différentielle de (k, D), on identifie k à un sous-corps de K et on note encore D pour Δ. Si $a \in k$, on écrira souvent $a\prime$ pour $D(a)$.

On dit que $t \in k$ est un logarithme de $a \in k^*$ si $t' = a'/a$.

On dit que $t \in k$ est une exponentielle de $a \in k$ si $t'/t = a'$.

On dit que $x \in k$ est une somme de Liouville dans k s'il existe $u \in k$, $v_1, ..., v_n \in k^*$, et $c_1, ..., c_n \in k_0$ tels que

$$x = u' + \sum_{i=1}^{n} c_i \frac{v_i'}{v_i}$$

Définition 2.2.2 *:*

Une extensoin différentielle (K, D) de (k, D) est dite élémentaire s'il existe une suite d'extensions

$$k = L_0 \subset L_1 \subset ... \subset L_n = K$$

vérifiant les conditions suivantes :

(1) K et k ont le même corps de constantes k_0.

(2) Pour $1 \leq j \leq n$, il existe $t_j \in L_j$ tel que $L_j = L_{j-1}(t_j)$ et t_j est algébrique sur L_{j-1}, ou un logarithme d'un élément de L_{j-1}, ou une exponentielle d'un élément de L_{j-1}.

Théorème 2.2.1 ***(Théorème de Liouville-Ostrowski).***

Soient (k, D) un corps différentiel et $x \in k$, s'il existe une extension élémentaire (K, D) de (k, D) et $y \in K$ vérifiant $y\prime = x$, alors x est une somme de Liouville dans k.

Définition 2.2.3 *:*

Soit (k, D) un corps différentiel, k_0 son corps des constantes est algébriquement clos et de caractéristique nulle.

Une équation différentielle linéaire homogène d'ordre n sur k est une équation de la forme

$$D^n(y) + a_{n-1}D^{n-1}(y) + ... + a_0 = 0 \tag{2.2.1}$$

avec $a_0, ..., a_{n-1} \in k$ et l'inconnue $y \in k$.

Si on pose $A = \begin{pmatrix} 0 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & . & . & . & 0 \\ . & . & . & & & & . \\ . & . & . & & & & . \\ . & . & . & & & & . \\ 0 & 0 & 0 & . & . & . & 1 \\ -a_0 & -a_1 & -a_2 & . & . & . & -a_{n-1} \end{pmatrix} \in M_n(k)$

$Y = {}^t\left(y, y', ..., y^{(n-1)}\right) \in M_{n,1}(k)$, on voit alors que y est une solution de l'équation (2.2.1) si et seulement si Y est solution de l'equation (E): $Y\prime = AY$

On dit qu'une extension différentielle (K, D) de (k, D) est une extension de Picard-Vessiot pour l'équation (E) si :

a) (E) admet une base de solutions $(Y_1, ..., Y_n)$ dans K

b) K est engendré par les coefficients Y_{ij} de cette base

c) Le corps des constantes de (K, D) est égal à k_0.

Théorème 2.2.2 *:*

(1) Toute équation différentielle admet une extension de Picard-Vessiot.

(2) Si $(K, \triangle)$ et (L, ∇) sont des extensions de Picard-Vessiot de (k, D) pour (E), il existe un k-isomorphisme $u : K \longrightarrow L$ tel que $u \circ \triangle = \nabla \circ u$

Définition 2.2.4 *:*

Soit (K, D) une extension de Picard-Vessiot de (k, D) pour (E).

Soit $(Y_1, ..., Y_n)$ une base du k_0 -espace vectoriel V des solutions de (E) dans K^n.

On appelle groupe de Galois différentiel de K sur k et on note $Gal^D(K/k)$, l'ensemble des automorphismes σ de K qui vérifient les conditions suivantes :

(1) $\sigma(x) = x$ pour tout $x \in k$.

(2) $[\sigma(y)]' = \sigma(y')$ pour tout $y \in K$.

$Gal^D(K/k) = \left\{\sigma : K \longrightarrow K \text{ tq } \forall x \in k : \sigma(x) = x \text{ et } \forall y \in K : \sigma(y') = \sigma(y)'\right\}$

De même que les groupes de Galois classiques sont des sous-groupes du groupe symétrique, le groupe de Galois différentiel est un sous-groupe du groupe $GL(V)$ des automorphismes k_0 -linéaires de V . (Remarque : $GL(V) \simeq GL_n(C)$.)

Proposition 2.2.1 *:*

Soit (K, D) une extension de Picard-Vessiot de (k, D) pour (E).

Soit $(Y_1, ..., Y_n)$ une base du k_0 -espace vectoriel V des solutions de (E) dans K^n.

(1) Si $\sigma \in Gal^D(K/k)$ pour toute solution Y de (E), $\sigma(Y)$ est une solution de (E).

(2) L'application $\sigma : V \longrightarrow V$ ainsi obtenue est un isomorphisme de k_0 -espace vectoriel.

(3) L'application $\varphi : Gal^D(K/k) \to GL_{k_0}(V)$ définie par $\sigma \longmapsto \sigma|_V$ est un homomorphisme injectif de groupes.

Preuve. : (1) Soit $\sigma \in Gal^D(K/k)$, soit $Y = {}^t(y_1, ..., y_n)$ une solution de (E). Montrons que $\sigma(Y)$ est une solution de (E), on a par hypothèse $Y\prime = AY$.

$$[\sigma(Y)]' = \sigma(Y') = \sigma(AY) = A\sigma(Y)$$

car σ est k-linéaire, d'où $\sigma(Y)$ est une solution de (E).

(2) l'application $\sigma : V \longrightarrow V$ ainsi obtenue est évidemment k_0 -linéaire car $k_0 \subset k$ donc l'application σ est un isomorphisme de k_0 -espaces vectoriels.

(3) Il faut montrer que si $\sigma \in Gal^D(K/k)$, vérifiant $\varphi(\sigma) = id$, alors $\sigma = id$.

Comme K est engendré sur k par les composantes des Y_j et comme

$\sigma|K = id_k$, on a $\sigma(y) = y$ pour tout $y \in K$, ce qui prouve que $\sigma = id$, ainsi φ est injectif.

■

Exemple 2.2.1 ***:(Logarithme)***

On munit $k = \mathbb{C}(X)$ de la dérivation usuelle D. On considère sur (k, D) l'équation différentielle non homogène $y\prime = \frac{1}{X}$, elle se transforme en une équation homogène

$$y" + \left(\frac{1}{X}\right) y\prime = 0 \tag{2.2.2}$$

On peut ramener (2.2.2) à l'équation matricielle suivante

$$Y' = \begin{pmatrix} 0 & 1 \\ 0 & -\frac{1}{X} \end{pmatrix} Y$$

Il est clair que $g = \alpha$ (en particulier $g = 1$) est solution de (2.2.2) .

Soit f une solution non constante de (2.2.2) ; alors (f, g) est libre sur $\mathbb{C}$ et forment une base de V, où V est l'espace vectoriel des solutions de l'equation (2.2.2) .

On peut montrer par l'absurde que f est transcendante sur $k = \mathbb{C}(X)$.

Alors $K = \mathbb{C}(X, Y)$ muni de la dérivation prolongeant D et telle que $Y\prime = \frac{1}{X}$ est une extension de Picard-Vessiot de (k, D) pour l'equation (2.2.2) .

La base (f, g) de V nous permet d'identifier $GL(V)$ et $GL_2(C)$. Soit $\sigma \in Gal^D(L/K)$ un automorphisme différentiel, comme $g = 1 \in k$, on a $\sigma(g) = g$. De plus, il existe a et $b \in \mathbb{C}$ tels que $\sigma(f) = af + bg$, en dérivant, on obtient $[\sigma(f)]\prime = af\prime = a/X$, alors que $[\sigma(f)]\prime = \sigma(f\prime) = 1/X$ nécessairement, $a = 1$ donc $\sigma(f) = f + bg$.

Enfin on obtient la restriction de σ dans V par :

$$\sigma \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix}$$

Donc le groupe de Galois différentiel de K sur k, $Gal^D(K/k)$ s'identifie au sous groupe T de $GL_2(C)$ defini par :

$$T = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} ; b \in \mathbb{C} \right\}$$

Chapitre 3

Solutions générales algébriques des équations différentielles ordinaires

3.1 Définitions de solutions générales algébriques :

On désigne par $K = \mathbb{Q}(x)$ le corps différentiel des fonctions rationnelles en x, muni de l'opérateur $\frac{d}{dx}$ et y est l'indéterminée sur K.

Soit $P \in K\{y\}$ un polynôme différentiel irréductible défini par :

$$P(y) = a_d y_k^d + a_{d-1} y_{k-1}^{d-1} + ... + a_0$$

où les a_i sont des polynômes en $y, y_1, ..., y_{k-1}$ et $a_d \neq 0$

L'initial de P est $I(P) = a_d$

Le séparent de P est $S = \frac{\partial P}{\partial y_k}$

L'ordre de P est $ord(p) = k$.

Soit l'ensemble $\Sigma_p = \{A \in K\{y\} / SA \equiv 0 \bmod, \{p(y)\}\}$ où $\{p(y)\}$ est l'idéal différentiel engendré par $p(y)$.

Remarque 3.1.1 *: Par le théorème 2.3, A est dans Σ_p, si A s'annule pour chaque zéro de P qui n'annule pas S.*

Lemme 3.1.1 *:*

Σ_p est un idéal différentiel premier et le polynôme différentiel Q appartient à Σ_p, si et seulement si, $prem\,(P,Q)=0$.

Preuve. : a) Montrons que Σ_p est un idéal.

Il est clair que la somme de deux polynômes différentiels dans Σ_p est contenu dans Σ_p.

En effet si $A,B\in\Sigma_p$, alors $SA\equiv 0\,\mathrm{mod}\,\{p\,(y)\}$ et $SB\equiv 0\,\mathrm{mod},\{p\,(y)\}$ et comme $S\,(A+B)=SA+SB$, alors $S\,(A+B)\equiv 0\,\mathrm{mod},\{p\,(y)\}$, donc $A+B\in\Sigma_p$.

De même pour le produit d'un polynôme différentiel dans Σ_p par un polynôme de $K\{y\}$, le produit est encore dans Σ_p.

En effet si $A\in\Sigma_p$ et $C\in K\,\{y\}$, on a : $SA\equiv 0\,\mathrm{mod}\,\{p\,(y)\}$ et comme $S\,(CA)=C\,(SA)$, alors $S\,(CA)\equiv 0\,\mathrm{mod}\,\{p\,(y)\}$, donc $CA\in\Sigma_p$.

b) Montrons que Σ_p est différentiel.

On montre que si A est dans Σ_p, alors A' est aussi dans Σ_p, où A' est la dérivée de A.

On a, A est dans Σ_p veut dire que SA est contenu dans $\{p\,(y)\}$ du lemme 2.1 du chapitre 2, il vient que SA' est contenu dans $\{p\,(y)\}$ d'où $SA'\equiv 0\,\mathrm{mod},\{p\,(y)\}$, donc $A'\in\Sigma_p$.

c) Montrons que Σ_p est premier.

Soit AB dans Σ_p, montrons que A ou B est contenu dans Σ_p.

Soit $ord\,(P)=k$, le procédé de réduction pour obtenir les formules du reste montre l'éxistence de :

$$S^bB\equiv T\,[P] \tag{3.1.1}$$

avec R et T d'ordre au plus k.

De (8) on obtient :

$$SRT\equiv S\,(S^aA)\left(S^bB\right),[P]$$

c'est àdire :

$$SRT\equiv S^{a+b+1}AB,[P]$$

Le second membre de cette congruence $S^{a+b+1}AB$ est contenu dans $\{p\,(y)\}$ car AB est dans Σ_p, alors le premier membre l'est aussi, d'où SRT est une combinaison linéaire de polynômes différentiels dans $\{p\,(y)\}$ et de leurs dérivées.

Soit alors :

$$(SRT)^c = MP + M_1P^{(1)} + ... + M_tP^{(t)}$$

d'aprés chapitre (2), on a :

$$P^{(t)} = Sy_{t+k} + R_t$$

où R_t est d'ordre au plus que $t + k$.

On remplace y_{t+k} dans $P^{(t)}$ et dans M par : $-\dfrac{R_t}{S}$, on obtieny la relation :

$$S^d\,(RT)^c = NP + N_1P^{(1)} + ... + N_{t-1}P^{(t-1)}$$

de proche en proche, on trouve que : $S^e\,(RT)^c$ est divisible par P.

Comme P est algébriquement irréductible, et n'est pas un facteur de S, donc P doit être un facteur d'au moins de R ou de T.

Supposons que R est divisible par P, de la formule (8), SA est contenu dans $\{p\,(y)\}$, d'où A est contenu dans Σ_p, ainsi Σ_p est un idéal premier.

d) Montrons que pour qu'un polynôme différentiel Q soit dans Σ_p, il est nécessaire et suffisant que le reste de Q par rapport à P soit égal à 0.

Soit Q un polynôme différentiel dans Σ_p, en divisant Q par P aura la relation :

$$S^aQ \equiv R\,[P] \tag{3.1.2}$$

où R est d'ordre au plus k.

De (9) on a :

$$SR \equiv S^a\,(SQ)\,,[P]$$

Comme $SQ \equiv 0\,[P]$, alors $SR \equiv 0\,[P]$, cela signifie que R est divisible par P, d'où le reste de Q par P est zéro.

Inversement si le reste de Q par P est égal à zéro, on a la relation (9) avec R est divisible par P, d'où Q est dans Σ ■

Comme conséquence du lemme précédent on a :

Lemme 3.1.2 *:*

Soit $F(y) \in K\{y\}$ un polynôme différentiel avec une solution générique η, alors pour un polynôme différentiel P, on a :

$$P(\eta) = 0 \text{ si et seulement si } prem(P, F) = 0$$

Définition 3.1.1 *:*

Soit $F(y) \in K\{y\}$ un polynôme différentiel irréductible, une solution générale algébrique de $F(y) = 0$ est définie comme une solution générale $\hat{y}$ qui satisfait l'équation suivante :

$$G(x, y) = \sum_{j=0}^{n} \sum_{i=0}^{m_j} a_{ij}\ x^i\ y^j = 0 \tag{3.1.3}$$

où les a_{ij} sont dans $\mathbb{C}$ et les est irréductible dans $\mathbb{C}[x, y]$

Remarque 3.1.2 *: Dans le cas où n=1 la relation (3.1.3) devient :*

$$\sum_{i=0}^{m_0} a_{i0} x^i + \sum_{i=0}^{m_1} a_{i1} x^i y = 0$$

et $\hat{y}$ est une solution générale rationnelle de $F(y) = 0$, qui s'écrit sous la forme :

$$\hat{y} = \frac{b_m x^m + ... + b_0}{x^p + c_{p-1} x^{p-1} + ... + c_0}$$

Pour les solutions algébriques de l'équation différentielle $F(y) = 0$, on a le lemme suivant :

Lemme 3.1.3 *:*

Soit $G(y) \in \mathbb{Q}(x)[y]$ et irréductible dans $\overline{\mathbb{Q}}(x)[y]$, où $\overline{\mathbb{Q}}$ est la clôture algébrique de $\mathbb{Q}$.

Si une solution de $G(y) = 0$ est une solution de $F(y) = 0$, alors toute solution de $G(y) = 0$ est une solution de $F(y) = 0$.

Preuve. :$G(y)$est irréductible dans $\overline{\mathbb{Q}}(x)[y]$, alors toute solution de $G(y) = 0$ est un zéro générique de $G(y) = 0$.

Du lemme 3.2, on a $prem(F, G) = 0$

On a :

$$S^k I^l F = PG' + QG \tag{3.1.4}$$

où $S = \dfrac{\partial G}{\partial y}$, I est l'initial de G, k et l sont dans $\mathbb{Z}$

Comme toute solution de $G(y) = 0$ est un zéro générique de $G(y) = 0$, et sachant que S et I ne s'annulent pas pour ce zéro, alors toute solution de $G(y) = 0$ est une solution de $F(y) = 0$. ■

Remarque 3.1.3 *: Dans la littérature, une solution générale de $F(y) = 0$ est définie comme une famille de solutions avec k paramétres indépendants, où $k = ord(F(y))$; la définition de Ritt est beaucoup plus précise.*

3.2 Un critère pour l'existence des solutions générales algébriques

Pour les entiers naturels h, α, k, on définit la matrice $A_{(h,\alpha,k)}(y)$ suivante :

$$\begin{pmatrix} \binom{k+1}{0} y_{k+1} & \binom{k+1}{1} y_k & . \ . \ . & \binom{k+1}{\alpha} y_{k+1-\alpha} \\ \binom{k+2}{0} y_{k+2} & \binom{k+2}{1} y_{k+1} & . \ . \ . & \binom{k+2}{\alpha} y_{k+2-\alpha} \\ . & . & . \ . \ . & . \\ . & . & . \ . \ . & . \\ . & . & . \ . \ . & . \\ \binom{k+h+1}{0} y_{k+h+1} & \binom{k+h+1}{1} y_{k+h+} & . \ . \ . & \binom{k+h+1}{\alpha} y_{k+h+1-\alpha} \end{pmatrix}$$

où $\binom{n}{k}$ sont les coefficients binomiaux, et si $k > n$, alors $\binom{n}{k} = 0$.

Soit $\underline{\alpha} = (\alpha_1, ..., \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ et $\alpha_0 \in \mathbb{Z}_{\geq 0}$ où $\mathbb{Z}_{\geq 0}$ est l'ensemble des entiers non négatifs.

Soit $A_{(\alpha_0:\underline{\alpha})}(y)$ la matrice $(h+1)(h+1)$ définie par :

$$A_{(\alpha_0:\underline{\alpha})}(y) = \left(A_{(h,\alpha_1:\alpha_0)}(y) / A_{(h,\alpha_2,\alpha_0)}\left(y^2\right) / ... / A_{(h,\alpha_n,\alpha_0)}\left(y^n\right)\right)$$

avec $n + \alpha_1 + ... + \alpha_n = h + 1$.

Soit $D_{(\alpha_0:\underline{\alpha})}$ le déterminant de $A_{(\alpha_0:\underline{\alpha})}(y)$

Remarquant que si $n = 1$, alors on se ramène au cas rationnelle car $D_{(\alpha_0:\underline{\alpha})} = D_{n,m}$.

Définition 3.2.1 *:*

Le wronskian des n éléments $y_1, y_2, ..., y_n$ dans un anneau différentiel F est le déterminant suivant :

$$W(y_1, y_2, ..., y_n) = \begin{vmatrix} y_1 & y_2 & . & . & . & y_n \\ y_1' & y_2' & . & . & . & y_n' \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ y_1^{(n-1)} & y_2^{(n-1)} & . & . & . & y_n^{(n-1)} \end{vmatrix}$$

Théorème 3.2.1 *:*

Soit F un corps différentiel, avec $\mathbb{C}$ son corps de constantes, alors les n éléments $y_1, y_2, ..., y_n$ sont linéairement dépendants sur $\mathbb{C}$ si et seulement si leur wronskian est nul.

Preuve. :Supposons que $y_1, y_2, ..., y_n$ sont linéairement dépendants sur $\mathbb{C}$.

Alors on a $c_1y_1 + c_2y_2 + ... + c_ny_n = 0$, avec les c_i ne sont pas tous nuls.

En dérivant cette équation $(n-1)$ fois, on trouve le système suivant de n équations linéaires homogénes de $c_1, c_2, ..., c_n$:

$$\sum c_i y_i^{(j)} = 0$$

où $\quad j = 0, ..., n-1$

Comme les c_i ne sont pas tous nuls, alors le déterminant de ce systéme doit être nul, d'où le wronskian est nul.

Inversement, supposons que le wronskian des éléments $y_1, y_2, ..., y_n$ est nul, alors on peut trouver dans F une solution non triviale parmi les solutions $c_1, c_2, ..., c_n$ des équations : $\sum c_i y_i^{(j)} = 0$; $j = 0, ..., n-1$.

Prenant $c_1 = 0$, le wronskian des éléments $y_2, y_3, ..., y_n$ n'est pas nul.

En dérivant les équations $\sum c_i y_i^{(j)} = 0$; $j = 0, ..., n-1$, et en éliminant la première équation obtenue, on aura les $(n-1)$ équations linéaires homogénes suivantes :

$$c_2' y_2^{(j)} + c_3' y_3^{(j)} + ... + c_n' y_n^{(j)} = 0$$

où $\quad j = 1, ..., n-1$

avec leur déterminant : le wronskian des éléments $y_2, y_3, ..., y_n$ qui n'est pas nul.

Alors $c_2' = c_3' = ... = c_n' = 0$, d'où les c_i sont constants, et les $y_1, y_2, ..., y_n$ sont linéairement dépendants ■

Lemme 3.2.1 *:*

Un élément $\overline{y}$ dans l'extension de K, est solution de l'équation $D_{(\alpha_0:\underline{\alpha})} = 0$ si et semlement si $\overline{y}$ satisfait l'équation (3.1.3) avec : $m_j \leq \alpha_j$ pour $j = 0, ..., n$

Preuve. : Supposons $\overline{y}$ satisfait l'équation (3.1.3) avec : $m_j \leq \alpha_j$ pour $j = 0, ..., n$

on a donc :

$$G(x, \overline{y}) = \sum_{j=0}^{n} \sum_{i=0}^{m_j} a_{ij} x^i \ \overline{y}^j = 0$$

$$\sum_{i=0}^{m_0} a_{i0} \ x^i + \sum_{j=1}^{n} \sum_{i=0}^{m_j} a_{ij} \ x^i \ \overline{y}^j = 0$$

comme $m_0 \leq \alpha_0$, alors

$$\sum_{i=0}^{m_0} a_{i0} \ \left(x^i\right)^{(\alpha_0+1)} = 0$$

et on aura :

$$\begin{aligned} G(x, \overline{y})^{(\alpha_0+1)} &= \sum_{j=0}^{n} \sum_{i=0}^{m_j} a_{ij} \left(x^i \ \overline{y}^j\right)^{(\alpha_0+1)} \\ &= \sum_{i=0}^{m_0} a_{i0} \left(x^i\right)^{(\alpha_0+1)} + \sum_{j=1}^{n} \sum_{i=0}^{m_j} a_{ij} \left(x^i \ \overline{y}^j\right)^{(\alpha_0+1)} \\ &= \sum_{j=1}^{n} \sum_{i=0}^{m_j} a_{ij} \left(x^i \ \overline{y}^j\right)^{(\alpha_0+1)} \end{aligned}$$

où $\left(x^i \ \overline{y}^j\right)^{(\alpha_0+1)}$ est la (α_0+1) dérivée de $\left(x^i \ \overline{y}^j\right)$ par rapport à x.

Comme $G(x,\overline{y})^{(\alpha_0+1)}=0$ et $a_{ij}=0$ pour $m_j<i\leq\alpha_j$, alors :

$$\sum_{j=1}^{n}\sum_{i=0}^{\alpha_j}a_{ij}\left(x^i\ \overline{y}^j\right)^{(\alpha_0+1)}=0$$

les éléments $\left(x^i\ \overline{y}^j\right)^{(\alpha_0+1)}$ pour $i=0,...,\alpha_j$ et $j=0,...,n$ sont linéairement dépendants sur $\mathbb{C}$ car les a_{ij} sont constants.

D'aprés le théorème 3.1, on aura leur wronskian nul

$$W\left(\left(x^i\ \overline{y}^j\right)^{(\alpha_0+1)}\right)=0\quad;\quad i=0,...,\alpha_j\ \text{ et }\ j=0,...,n$$

d'autre part

$$W\left(\left(x^i\ \overline{y}^j\right)^{(\alpha_0+1)}\right)=D_{(\alpha_0:\underline{\alpha})}(\overline{y})\times|diag(B_0,B_1,...,B_n)|$$

où $diag(B_0,B_1,...,B_n)$ est la matrice diagonale des B_j pour $j=0,...,n$

$$B_j=\begin{pmatrix}1&x&x^2&.&.&.&x^{\alpha_j}\\0&1&2x&.&.&.&\alpha_j x^{\alpha_j-1}\\0&0&2&.&.&.&.\\.&.&.&.&.&.&.\\.&.&.&.&.&.&.\\0&0&0&.&.&.&\alpha_j!\end{pmatrix}$$

$W\left(\left(x^i\ \overline{y}^j\right)^{(\alpha_0+1)}\right)=0$ équivaut à $D_{(\alpha_0:\underline{\alpha})}(\overline{y})=0$.

D'où $G(x,\overline{y})=0$ équivaut à $D_{(\alpha_0:\underline{\alpha})}(\overline{y})=0$, avec $m_j\leq\alpha_j$ pour $j=0,...,n$ ■

Théorème 3.2.2 *:*

Soit F un polynôme différentiel irréductible, l'équation $F=0$ a une solution générale algébrique si et seulement si il existe $\underline{\alpha}=(\alpha_1,...,\alpha_n)\in\mathbb{Z}_{\geq 0}^n$ et $\alpha_0\in\mathbb{Z}_{\geq 0}$ tels que : $prem\left(D_{(\alpha_0:\underline{\alpha})},F\right)=0$.

Preuve. : On suppose que $\overline{y}$ est une solution générale algébrique de l'équation $F=0$, qui satisfait (3.1.3) et soit $\underline{\alpha}=(m_1,...,m_n)$ et $\alpha_0=m_0$ d'aprés lemme 3.4 on a : $D_{(\alpha_0:\underline{\alpha})}(\overline{y})=0$, et d'aprés lemme 3.1 et lemme 3.2 on a :$D_{(\alpha_0:\underline{\alpha})}\in\sum_F$, et donc : $prem\left(D_{(\alpha_0:\underline{\alpha})},F\right)=0$.

Réciproquement, on suppose que $prem\left(D_{(\alpha_0:\underline{\alpha})}, F\right) = 0$, cela signifie que $D_{(\alpha_0:\underline{\alpha})} \in \sum_F$, d'aprés lemme 3.1, alors tous les zéros de $\sum_F$ doivent vérifier l'équation (3.1.3) , en particulier le zéro générique de $\sum_F$ vérifie l'équation (3.1.3) . ■

Chapitre 4

Solutions générales algébriques d'équations différentielles du premier ordre

Dans ce chapitre, $F(y)$ est un polynôme différentiel non nul, du premier ordre dans $\mathbb{Q}\{y\}$et irréductible dans $\overline{\mathbb{Q}}\{y\}$et $G(x,y)$ est un élément de $\overline{\mathbb{Q}}[x,y]$.

On dira que $G(x,y)$ est non triviale si $deg(G,x) > 0$ et $deg(G,y) > 0$; dans ce qui suit, on suppose que $G(x,y)$ est non triviale.

On dira que $G(x,y) = 0$ est une solution algébrique de $F = 0$ équivaut à dire que l'une des fonctions algébriques $\hat{y}(x)$ définie par $G(x,\hat{y}(x)) = 0$ est une solution de $F = 0$.

4.1 Structure et degré des solutions générales algébriques

Pour une équation différentielle ordinaire, une solution est invariante par une translation de la variable x, on a donc le lemme

Lemme 4.1.1 *:*

Soit $G(x,y) = 0$ une solution algébrique de $F = 0$, alors $G(x+c,y) = 0$ est une solution générale algébrique de $F = 0$ où c est une constante arbitraire.

Preuve. : Il faut montrer que si $\overline{y}(x)$ est une série formelle solution de $G(x,y)=0$, alors $\overline{y}(x+c)$ est une série formelle solution de $G(x+c,y)=0$

Pour tout $T \in K\{y\}$ satisfaisant $T(\overline{y}(x+c))=0$, soit $R=prem(T,F)$

On montre par l'absurde que $R(\overline{y}(x+c))=0$.

Supposons que $R \neq 0$, on a F est irréductible et $deg(R,y_1) < deg(F,y_1)$, alors il existe deux polynômes P et Q dans $K\{y\}$ tels que $(PF+QR) \in K\{y\}$ et $PF+QR \neq 0$.

D'autre part $(PF+QR)(\overline{y}(x+c))=0$ parceque $\overline{y}(x+c) \notin \overline{\mathbb{Q}}$ et c est une constante arbitraire qui est transcendante sur K, on a donc $(PF+QR)=0$, d'où une contradiction, donc $R=0$, ce qui signifie que $T \in \sum_F$, donc $\overline{y}(x+c)$ est un zéro générique de $\sum_F$, alors $G(x+c,y)=0$ est une solution algébrique de l'équation $F=0$. ■

Le lemme ci dessus, réduit le calcul d'une solution générale algébrique à un calcul d'une solution algébrique particulière non triviale.

Dans ce qui suit, on montrera comment calculer une solution algébrique non triviale dans $\overline{\mathbb{Q}}[x,y]$.

Définition 4.1.1 *:*

Le corps § est appellé corps d'une fonction algébrique d'une seule variable si x transcendant sur § et α algébrique sur $\overline{\mathbb{Q}}(x)$.

Une courbe algébrique irréductible $G(x,y)=0$ où $G(x,y) \in \overline{\mathbb{Q}}[x,y]$, correspond à un corps d'une fonction algébrique § qui est unique, à un isomorphisme près, où $(\alpha\ ,\beta)$ satisfait $G(\alpha,\beta)=0$ et α ou β est transcendant sur §.

Notons que deux courbes algébriques isomorphes à § fonction algébrique, ont le même genre. .

Définition 4.1.2 *:*

Soit $G(x,y)$ un polynôme non trivial et irréductible dans $\overline{\mathbb{Q}}[x,y]$, on dira que $(x(t),y(t))$ est une paramétrisation de $G(x,y)=0$ si $G(x(t),y(t))=0$ où $x(t),y(t) \in \overline{\mathbb{Q}}((t))$ et non tous dans $\overline{\mathbb{Q}}$. Rappellons que $\overline{\mathbb{Q}}((t))$ est le corps quotient de l'anneau des séries formelles $\overline{\mathbb{Q}}[[t]]$.

Il existe donc $x_0, y_0 \in \overline{\mathbb{Q}}$ et deux entiers non nuls q et p et $u(t)$, $v(t)$ dans $\overline{\mathbb{Q}}[[t]]$ tels que :

$$\left\{ \begin{array}{l} x(t) = x_0 + t^q.u(t) \\ y(t) = y_0 + t^p.v(t) \end{array} \right\} \tag{4.1.1}$$

Le centre de cette paramétrisation est le point $P \in P^1 \times P^1$ défini par :

a) Si $q > 0$ et $p > 0$ alors $P = (x_0, y_0)$

b) Si $q > 0$ et $p < 0$ alors $P = (x_0, \infty)$

c) Si $q < 0$ et $p > 0$ alors $P = (\infty, y_0)$

d) Si $q < 0$ et $p < 0$ alors $P = (\infty, \infty)$

Si $q < 0$ (respectivement $p < 0$) on suppose que $x_0 = 0$ (respectivement $y_0 = 0$).

La paramétrisation est dite réductible s'il existe un entier $k \geq 2$ tel que $x(t), y(t) \in \overline{\mathbb{Q}}\left(\left(t^k\right)\right)$, sinon elle est irréductible.

$\left(x\left(\bar{t}\right), y\left(\bar{t}\right)\right)$ est une autre paramétrisation de $G(x,y) = 0$ de même centre, si $\bar{t} \in \overline{\mathbb{Q}}[[t]]$ avec un ordre plus grand que zéro.

Si l'ordre de $\bar{t}$ est égal à 1, les deux paramétrisations sont dites équivalentes, et ont les mêmes entiers q et p définies ci-dessus. B est dite la place de la courbe $G(x,y) = 0$, si B est l'ensemble des paramétrisations irréductibles équivalentes; le centre de B est le centre de l'une de ses paramétrisations irréductibles.

On définit les entiers $V_x(B)$ et $V_y(B)$ comme suit :

$$V_x(B) = q \text{ et } V_y(B) = p$$

Par la suite, on aura besoin de la formule de Riemann-Herwitz et les expressions des séries de Puiseux.

Formule de Riemann-Herwitz :

Soit g le genre de $G(x,y) = 0$ et $n = deg(G,y)$ alors :

$$g = 1 - n + \frac{1}{2}\sum_B \left(|V_x(B)| - 1\right)$$

où la somme parcourt toutes les places B de la courbe $G(x,y) = 0$.

Expressions des séries de Puiseux :

Toute place B de centre (x_0, y_0) correspond exactement aux q_B séries fractionnelles $y\left(x^{\frac{1}{q_B}}\right)$ qui sont solutions de $G(x,y)=0$.

Soit $x_0 \in \overline{\mathbb{Q}} \cup \{\infty\}$, on a les types de séries de Puiseux :

1) Séries de Puiseux pour $x_0 \in \overline{\mathbb{Q}}$:

$$\begin{aligned} a)\ y-y_0 &= a_1 (x-x_0)^{\frac{p}{q_i}} + \sum_{i\geq 1} a_i (x-x_0)^{\frac{i+p}{q_i}} \\ b) \qquad y &= a_{-p} (x-x_0)^{-\frac{p}{q_i}} + \sum_{i\geq 1} a_i (x-x_0)^{\frac{i-p}{q_i}} \end{aligned}$$

2) Séries de Puiseux pour $x_0 \in \infty$:

$$\begin{aligned} a)\ y-y_0 &= a_1 \left(\frac{1}{x}\right)^{\frac{p}{q_i}} + \sum_{i\geq 1} a_i \left(\frac{1}{x}\right)^{\frac{i+p}{q_i}} \\ b) \qquad y &= a_{-p} \left(\frac{1}{x}\right)^{-\frac{p}{q_i}} + \sum_{i\geq 1} a_i \left(\frac{1}{x}\right)^{\frac{i-p}{q_i}} \end{aligned}$$

où $a_i \in \overline{\mathbb{Q}}$ et p et $q_i \in \mathbb{Z}_{>0}$, $q_i > 1$.

D'aprés théorème de Puiseux, on a

$$\sum_B |V_x(B)| = \deg(G, y) \tag{4.1.2}$$

où la somme parcourt toute les places B de la courbe $G(x,y)=0$.

Lemme 4.1.2 *:*

Soit $G(x,y)$ un polynôme irréductible, non trivial dans $\overline{\mathbb{Q}}[x,y]$ et soit $(x(t), y(t))$ une paramétrisation de $G(x,y)=0$, alors $(x(t)+c, y(t))$ n'est pas une paramétrisation de $G(x,y)=0$, pour toute constante non nulle $c \in \overline{\mathbb{Q}}$

Preuve. : D'aprés le lemme de Gauss, on sait que $G(x,y)$ est irréductible dans $\overline{\mathbb{Q}}(y)[x]$ comme $y(t) \notin \overline{\mathbb{Q}}$, alors $\overline{\mathbb{Q}}(y(t))$ est isomorphe à $\overline{\mathbb{Q}}(y)$, ce qui implique que $G(x, y(t))$ est irréductible dans $\overline{\mathbb{Q}}(y(t))[x]$.

Supposons que $x(t)$ est une racine de $G(x+c, y(t))=0$, alors on a $G(x, y(t))$ divise $G(x+c, y(t))$, il est clair que $\deg(G(x+c, y(t)), x) = \deg(G(x, y(t)), x)$ et $G(x, y(t)) ; G(x+c, y(t))$

ont les mêmes coefficients, donc $G(x, y(t)) = G(x + c, y(t))$.et comme $c \neq 0$, on a $\deg(G(x, y(t)), x) = \deg(G(x, y), x) = 0$: contradiction. ■

Théorème 4.1.1 *:*

Soit $G(x, y)$ un polynôme irréductible, non trivial dans $\overline{\mathbb{Q}}[x, y]$ et $G(x, y) = 0$ est la solution de l'équation $F = 0$, alors on a :

$$\deg(G, x) = \deg(F, y_1) \tag{4.1.3}$$

Preuve. :Soit $\deg(G, x) = s$ et $\deg(F, y_1) = d$

On peut écrire :

$$\begin{aligned} G(x, y) &= A_0(y) + A_1(y)\, x + ... + A_s(y)\, x^s \\ F(y) &= F_0(y) + F_1(y)\, y_1 + ... + F_d(y)\, y_1^d \end{aligned}$$

où les $A_i(y)$ et les $F_j(y)$ sont dans $\overline{\mathbb{Q}}[y]$.

Soit S l'ensemble : $S = Z(A_s(y)) \cup Z(F_d(y)) \cup Z\left(Res_x\left(G, \frac{\partial G}{\partial x}\right)\right) \cup Z\left(Res_x\left(G, \frac{\partial G}{\partial y}\right)\right) \cup Z\left(Res_{y_1}\left(F, \frac{\partial F}{\partial y_1}\right)\right)$

S est un ensemble fini, alors on peut choisir $c \in \overline{\mathbb{Q}}$ tel que $c \notin S$; on a donc les résultats suivants :

a) L'ensemble $\left\{z \in \overline{\mathbb{Q}} / F(c, z) = 0\right\} = \{z_1, z_2, ..., z_d\}$ a d éléments.

b) L'ensemble $\left\{x \in \overline{\mathbb{Q}} / G(x, c) = 0\right\} = \{x_1, x_2, ..., x_s\}$ a s éléments.

c) Comme $\dfrac{\partial G}{\partial y}(x_i, c) \neq 0$, alors il existe une unique série formelle

$$\varphi_i(x) = c + g_{i,1}(x - x_i) + g_{i,2}(x - x_i)^2 + ...$$

tels que $G(x, \varphi_i(x)) = 0$ pour $i = 1, ..., s$.

Du lemme 3.3, $\varphi_i(x)$ est une solution de $F = 0$, alors on a :

$$F(\varphi_i(x), \varphi_i'(x)) = 0$$

ce qui implique que $F(c, g_{i,1}) = 0$ car $\varphi_i(x_i) = c$ et $\varphi_i'(x_i) = g_{i,1}$.

Supposons que : $s > d$, alors il existe au moins deux des $g_{i,1}$ qui sont égaux, posons $g_{1,1} = g_{2,1} = c_1$, comme $\dfrac{\partial F}{\partial y_1}(c, c_1) \neq 0$, alors il existe une unique solution $\varphi(x)$ de $F(y, y_1) = 0$ qui vérifie $\varphi(0) = c$ et $\varphi'(0) = c_1$, alors $\varphi_1(x) = \varphi_2(x + x_2 - x_1) = \varphi(x - x_1)$

donc $(x, \varphi_1(x))$ et $(x + x_2 - x_1, \varphi_1(x))$ sont deux paramétrisations de $G = 0$, d'où une contradiction avec le lemme 4.2, donc : $s \leq d$.

D'autre part :

$$\begin{aligned} G' &= \frac{\partial y}{\partial x}.\frac{\partial G}{\partial y} + \frac{\partial x}{\partial x}.\frac{\partial G}{\partial x} \\ &= y_1.\frac{\partial G}{\partial y} + \frac{\partial G}{\partial x} \end{aligned}$$

et soit $H(y, y_1) = Res_x(G, G')$, alors

$$\begin{aligned} H(y, y_1) &= Res_x\left(G, y_1.\frac{\partial G}{\partial y} + \frac{\partial G}{\partial x}\right) \\ &= Res_x\left(G, y_1.\frac{\partial G}{\partial y}\right) + M(y_1) \\ &= y_1^s Res_x\left(G, \frac{\partial G}{\partial y}\right) + M(y_1) \end{aligned}$$

où $\deg(M, y_1) < s$, comme $Res_x\left(G, \frac{\partial G}{\partial y}\right) \neq 0$, on a donc $\deg(H(y, y_1), y_1) = s$.

Supposons que $\overline{y}(x)$ est une solution de $G(x, y) = 0$, alors on a :

$$H(\overline{y}(x), \overline{y}'(x)) = F(\overline{y}(x), \overline{y}'(x))$$

et comme F est irreductible, on a $\deg(H(y, y_1), y_1) \geq \deg(F(y, y_1), y_1)$, d'où $s \geq d$, donc $s = d$. ■

Remarquons que F est du premier ordre, donc on peut regarder $F = 0$ comme une courbe algébrique et on utilise la notation F designe $F(y, y_1)$

Lemme 4.1.3 *:*

Soit $G(x, y) = 0$ une solution de $F = 0$, alors le genre de $G(x, y) = 0$ est égale au genre de $F(y, y_1) = 0$.

Preuve. : Soit α qui vérifie $G(x, \alpha) = 0$, donc α est transcendant dans $\overline{Q}$ et $\overline{Q}(x, \alpha), \overline{Q}(\alpha, \alpha')$ sont les corps des fonctions algébriques de $G(x, y) = 0, F(y, y_1) = 0$, respectivement.

Il reste à montrer que $\overline{Q}(x,\alpha) = \overline{Q}(\alpha,\alpha')$.

D'aprés théorème précédent on a :

$$\left[\overline{Q}(x,\alpha) : \overline{Q}(\alpha)\right] = \left[\overline{Q}(\alpha,\alpha') : \overline{Q}(\alpha)\right]$$

Comme $G(x,\alpha) = 0$, alors $G'(x,\alpha) = 0$.

$$\begin{aligned} G'(x,\alpha) &= y_1.\frac{\partial G(x,\alpha)}{\partial y} + \frac{\partial G(x,\alpha)}{\partial x} \\ \text{alors} \quad 0 &= \alpha'.\frac{\partial G(x,\alpha)}{\partial y} + \frac{\partial G(x,\alpha)}{\partial x} \\ \text{donc} \quad \alpha' &= -\frac{\frac{\partial G(x,\alpha)}{\partial x}}{\frac{\partial G(x,\alpha)}{\partial y}} \end{aligned}$$

ce qui implique que $\alpha' \in \overline{Q}(x,\alpha)$, d'où $\overline{Q}(x,\alpha) = \overline{Q}(\alpha,\alpha')$. ■

Par convention, on considère la nouvelle équation différentielle :

$$\overline{F}(x_1,y) = x_1^{\deg(F,y_1)}.F\left(y,\frac{1}{x_1}\right) = 0 \tag{4.1.4}$$

où $x_1 = \dfrac{dx}{dy} = \dfrac{1}{y_1}$, $\overline{F}$ est irréductible dans $\overline{\mathbb{Q}}[x_1,y]$ et $\deg\left(\overline{F},y\right) = \deg(F,y)$ et $\deg\left(\overline{F},x_1\right) = \deg(F,y_1)$.

Lemme 4.1.4 *:*

Soit F définie dans (4.1.4) et $G(x,y) = 0$ est une solution algébrique de $F(y,y_1) = 0$, alors $G(x,y) = 0$ est aussi une solution algébrique de $\overline{F}(x_1,y) = 0$.

Preuve. : D'aprés la preuve du théorème 4.1 on sait que :

$$\begin{aligned} Res_x(G,G') &= A(y).F(y,y_1) \\ \text{où} \quad G' &= y_1.\frac{\partial G}{\partial y} + \frac{\partial G}{\partial x} \end{aligned}$$

D'autre part, il existe deux polynômes $P,Q \in \overline{\mathbb{Q}}[x,y,y_1]$ tels que :

$$\begin{aligned} PG + QG' &= A(y).F(y,y_1) \\ PG + Q\left(y_1.\frac{\partial G}{\partial y} + \frac{\partial G}{\partial x}\right) &= A(y).F(y,y_1) \end{aligned}$$

L'expression (4.1.4) nous donne

$$F(y, y_1) = \overline{F}(x_1, y) .x_1^{-\deg(F,y_1)}$$

alors :

$$PG + Q\left(y_1.\frac{\partial G}{\partial y} + \frac{\partial G}{\partial x}\right) = A(y) .\overline{F}(x_1, y) .x_1^{-\deg(F,y_1)}$$

remplaçons y_1 par $\dfrac{1}{x_1}$ et multiplions les deux membres par x_1, on obtient :

$$\begin{aligned}(x_1P) G + x_1Q\left(\frac{1}{x_1}.\frac{\partial G}{\partial y} + \frac{\partial G}{\partial x}\right) &= A(y) .\overline{F}(x_1, y) .x_1^{1-\deg(F,y_1)} \\ P_1G + Q\left(\frac{\partial G}{\partial y} + x_1\frac{\partial G}{\partial x}\right) &= A(y) .\overline{F}(x_1, y) .x_1^{1-\deg(F,y_1)}\end{aligned}$$

En multiplions les deux membres de cette dernière égalité par x_1^m on aura :

$$\overline{P}G + \overline{Q}\left(\frac{\partial G}{\partial y} + x_1\frac{\partial G}{\partial x}\right) = A(y) .\overline{F}(x_1, y) .x_1^k \tag{4.1.5}$$

où $\overline{P}, \overline{Q} \in \overline{\mathbb{Q}}[x, y, y_1]$ et $k \in \mathbb{Z}_{\geq 0}$

On suppose que β satisfait $G(\beta, y) = 0$, remplaçons x par β et x_1 par β' dans l'égalité (4.1.5) où $\beta' = \frac{\partial \beta}{\partial y}$, on aura donc $\overline{F}(\beta', y) = 0$, d'où $G(x, y) = 0$ est aussi une solution algébrique de $\overline{F}(x_1, y) = 0$. ■

Lemme 4.1.5 *:*

Soit $(x(t), y(t))$ une paramétrisation irréductible de $G = 0$, alors $\left(\dfrac{x'(t)}{y'(t)}, y(t)\right)$ est une paramétrisation irréductible de $\overline{F}(x_1, y) = 0$.

Preuve. : D'aprés lemme 4.4 $\overline{F}(x_1(t), y(t)) = 0$
comme $x_1(t) = \dfrac{dx}{dy}(t)$, alors $x_1(t) = \dfrac{x'(t)}{y'(t)}$ où $x'(t) = \dfrac{dx}{dt}$ et $y'(t) = \dfrac{dy}{dt}$
on aura donc :

$$\overline{F}\left(\frac{x'(t)}{y'(t)}, y(t)\right) = 0$$

alors $\left(\frac{x'(t)}{y'(t)}, y(t)\right)$ est une paramétrisation de $\overline{F}(x_1, y) = 0$.
Montrons par l'absurde que $\left(\frac{x'(t)}{y'(t)}, y(t)\right)$ est irréductible.

On suppose qu'elle est réductible, alors il existe $k \geq 2$ tel que $x_1(t), y(t) \in \overline{\mathbb{Q}}\left(\left(t^k\right)\right)$ on aura donc :

$$x_1(t).y'(t) = \sum_{j \geq j_0} c_j t^{kj-1}$$

et comme $x_1(t).y'(t) = x'(t)$ alors :

$$= \sum_{j \geq j_0} c_j t^{kj-1}$$

en intégrant par rapport à t on obtient :

$$x(t) = \sum_{j \geq j_0} \frac{c_j}{kj} t^{kj} + c$$

où c est une constante: d'où une contradiction car $x(t) \in \overline{\mathbb{Q}}\left(\left(t^k\right)\right)$.
Donc $\left(\dfrac{x'(t)}{y'(t)}, y(t)\right)$ est une paramétrisation irréductible de $\overline{F}(x_1, y) = 0$. ■

Théorème 4.1.2 *:*

Soit $G(x, y)$ un polynôme irréductible et non trivial dans $\overline{\mathbb{Q}}[x, y]$ et $G(x, y) = 0$ est la solution de l'équation $F(y, y_1) = 0$ alors on a :

$$\deg(G, y) \leq \deg(F, y) + \deg(F, y_1) \tag{4.1.6}$$

Preuve. : Soient g_G et $g_{\overline{F}}$ respectivement les genres de $G(x, y) = 0$ et $\overline{F}(x_1, y) = 0$, et soit B la place de $G(x, y) = 0$ de centre $P(\alpha, \beta)$ avec sa paramétrisation irréductible $(x(t), y(t))$ et soit $\overline{B}$ la place de la courbe algébrique $\overline{F}(x_1, y) = 0$ de centre $\overline{P}\left(\overline{\alpha}, \overline{\beta}\right)$ avec sa paramétrisation irréductible $(x_1(t), y(t))$ où $x_1(t) = \dfrac{x'(t)}{y'(t)}$, il est clair que : $V_y(B) = V_y\left(\overline{B}\right)$ et $\beta = \overline{\beta}$.

$\diamond$ Si $V_x(B) \neq V_y(B)$ alors

$$V_{x_1}\left(\overline{B}\right) = V_x(B) - V_y(B)$$

- d'où si : $V_x(B) > V_y(B)$, alors $\overline{\alpha} = 0$
- Si : $V_x(B) < V_y(B)$alors $\overline{\alpha} = \infty$.

$\diamond$ Si $V_x(B) = V_y(B)$ alors $\overline{\alpha} \in \overline{\mathbb{Q}}$.

L'application qui associe à toute place B de $G(x,y)=0$, la place $\overline{B}$ de $\overline{F}(x_1,y)=0$ est injective.

En effet, soient B et B' deux places de $G(x,y)=0$ telles que $\overline{B}=\overline{B'}$ et soient $(x(t), y(t))$ et $(z(t), v(t))$ les paramétrisations de B et B' respectivement, on a alors :

$$y(t) = y_0 + t^p \text{ et } v(t) = v_0 + t^{p'}$$

comme $\overline{B}=\overline{B'}$ donc $p=p'$, $y(t)=v(t)$ et $x'(t)=z'(t)$, alors $z(t)=x(t)+c$, où c est constante.

D'aprés lemme 4.2 on a $c=0$, d'où $B=B'$.

D'autre part, on a d'après formule de Riemann- Herwitz :

$$2(g_G + \deg(G,y) - 1) = \sum_B (|V_x(B)| - 1)$$

où la somme parcourt toutes les places B de $G=0$.

On va exprimer la somme du second membre de l'égalité précédente comme suit :

On dit que :

$$\begin{aligned} B &\in (1) \text{ si } V_x(B) > 0 \text{ et } V_y(B) > 0 \\ B &\in (2) \text{ si } V_x(B) > 0 \text{ et } V_y(B) < 0 \\ B &\in (3) \text{ si } V_x(B) < 0 \text{ et } V_y(B) > 0 \\ B &\in (3) \text{ si } V_x(B) < 0 \text{ et } V_y(B) < 0 \end{aligned}$$

On dira aussi que :

$$\begin{aligned} B &\in (1') \text{ si } B \in (1) \text{ et } V_x(B) > V_y(B) \\ B &\in (4') \text{ si } B \in (4) \text{ et } V_x(B) < V_y(B) \end{aligned}$$

Dans ce qui suit $B_x, B_y, \overline{B}_{x_1}, \overline{B}_y$ designent respectivement :$V_x(B), V_y(B), V_{x_1}\left(\overline{B}\right), V_y\left(\overline{B}\right)$.

Pour $k=1$ et $k=4$ on a :

$$\sum_{B\in(k)} (|B_x| - 1) \leq \sum_{B\in(k')} \left|\overline{B}_{x_1}\right| + \sum_{B\in(k)} \left(\left|\overline{B}_y\right| - 1\right) \tag{4.1.7}$$

Pour $k = 2$ et $k = 3$ on a :

$$\sum_{B\in(k)} (|B_x| - 1) \leq \sum_{B\in(k)} \left|\overline{B}_{x_1}\right| \tag{4.1.8}$$

en ajoutant les inégalités (4.1.7) et(4.1.8) membre à membre, on obtient:

$$\sum_{B\in(k)} (|B_x| - 1) \leq \sum_{B\in(1'),(4'),(2),(3)} \left|\overline{B}_{x_1}\right| + \sum_{B\in(1),(4)} \left(\left|\overline{B}_y\right| - 1\right) \tag{4.1.9}$$

D'autre part si $B \in (1)' \cup (2)$ alors le centre de $\overline{B}$ est sur $x_1 = 0$.

si $B \in (4)' \cup (3)$ alors le centre de $\overline{B}$ est sur $x_1 = \infty$.

et en utilisant la formule (4.1.2) , on aura :

$$\sum_{B\in(1'),(4'),(2),(3)} \left|\overline{B}_{x_1}\right| \leq 2\deg\left(\overline{F}, y\right) \tag{4.1.10}$$

d'aprés la formule de Riemann- Herwitz, on a :

$$2\left(g_{\overline{F}} + \deg\left(\overline{F}, x_1\right) - 1\right) = \sum_{\overline{B}} \left(\left|V_y\left(\overline{B}\right)\right| - 1\right)$$

et comme :

$$\sum_{B\in(1),(4)} \left(\left|V_y\left(\overline{B}\right)\right| - 1\right) \leq \sum_{\overline{B}} \left(\left|V_y\left(\overline{B}\right)\right| - 1\right)$$

alors :

$$\sum_{B\in(1),(4)} \left(\left|\overline{B}_y\right| - 1\right) \leq 2\left(g_{\overline{F}} + \deg\left(\overline{F}, x_1\right) - 1\right) \tag{4.1.11}$$

En utilisant les inégalités)4.1.9(,)4.1.10(et)4.1.11(on aura :

$$\sum_{B\in(k)} (|B_x| - 1) \leq 2\left(\deg\left(\overline{F}, y\right) + g_{\overline{F}} + \deg\left(\overline{F}, x_1\right) - 1\right)$$

et comme :

$$\sum_{B\in(k)} (|B_x| - 1) = 2\left(g_G + \deg\left(G, y\right) - 1\right)$$

on aura :

$$2\left(g_G + \deg\left(G, y\right) - 1\right) \leq 2\left(\deg\left(\overline{F}, y\right) + g_{\overline{F}} + \deg\left(\overline{F}, x_1\right) - 1\right)$$

et en utilisant $\deg\left(\overline{F}, y\right) = \deg\left(F, y\right)$, $\deg\left(\overline{F}, x_1\right) = \deg\left(F, y_1\right)$ et $g_G = g_{\overline{F}}$, la dernière inégalité sera donc :

$$\deg\left(G, y\right) \leq \deg\left(F, y\right) + \deg\left(F, y_1\right)$$

. ■

Exemple 4.1.1 *:*

Soient $n > m > 0$ et $\gcd(n, m) = 1$ et soit $G(x, y) = y^n - x^m$ un polynôme irréductible.

On a $G(x, y) = 0$ est une solution algébrique de l'équation différentielle $F = 0$ où $F = y^{n-m} y_1^m - \left(\frac{m}{n}\right)^m$.

Dans ce cas, on a :

$$\deg(G, y) = \deg(F, y) + \deg(F, y_1)$$

4.2 Un algorithme pour le calcul des solutions algébriques

L'algorithme suivant est basé sur l'approximation algébrique, qui est un type spécial de l'approximation de Padé-Hermitz, pour cela on va donner quelques lemmes et définitions.

Définition 4.2.1 *:*

Soit la série formelle $A(x) = \sum_0^\infty a_i x^i$ et soit L et M deux entiers non négatifs.

Le (L, M) Padé-approximation de $A(x)$ est la fraction rationelle :$[L \setminus M] = \frac{P_L(x)}{Q_M(x)}$ telle que

$$A(x) - \frac{P_L(x)}{Q_M(x)} = 0\left(x^{L+M+1}\right)$$

où : $P_L(x)$ est un polynôme de degré inférieur ou égal à L.

$Q_M(x)$ est un polynôme de degré inférieur ou égal à M.

Notons que cette approximation est unique (d'après Frobenius et Padé) .

Définition 4.2.2 *:*

Soit $G(x, y)$ un polynôme irréductible dans $\overline{\mathbb{Q}}[x, y]$, une fonction algébrique $\overline{y}(x)$ satisfaisant $G(x, \overline{y}(x)) = 0$ est dite approximation algébrique d'une fonction $f(x)$ si :

$$G(x, f(x)) = 0\left(x^{(m+1)(n+1)+1}\right)$$

où $m = \deg(G, x)$ et $n = \deg(G, y)$

Plus généralement on cherche $G(x,y)$ telle que :

$$G(x, f(x)) = 0\left(x^{N+1}\right) \tag{4.2.1}$$

où N est un entier positif.

On peut trouver les coefficients de $G(x,y)$ par résolution d'équations linéaires
Soit $G(x,y) = \sum_{j=0}^{n}\sum_{i=0}^{m} b_{ij}\ x^i\ y^j$ et $f(x) = a_0 + a_1x + ... + a_Nx_N + 0\left(x^{N+1}\right)$.
Soit M_0 la matrice $(N+1)(m+1)$ définie par :

$$M_0 = \begin{pmatrix} I_{(m+1)(m+1)} \\ 0_{(N-m)(m+1)} \end{pmatrix} \tag{4.2.2}$$

où $I_{(m+1)(m+1)}$ est une matrice carrée à $(m+1)$ unité et $0_{(N-m)(m+1)}$ est une matrice à $(N-m)(m+1)$ zéros et on définit les matrices M_i par $M_i = TM^i \times M_0$ pour $i = 1, ..., n$, où TM est la matrice :

$$TM = \begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 \\ a_1 & a_0 & 0 & \cdots & 0 \\ a_2 & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_N & a_{N-1} & a_{N-2} & \cdots & a_0 \end{pmatrix} \tag{4.2.3}$$

Chaque matrice M_i est une matrice $(N+1) \times (m+1)$.

L'équation (4.2.1) s'écrira d'une autre façon :

$$(M_0 | M_1 | M_2 | ... | M_n) \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix} = 0 \text{ , où } B_i = \begin{pmatrix} b_{0,i} \\ b_{1,i} \\ b_{2,i} \\ \vdots \\ b_{n,i} \end{pmatrix} \text{ pour } i = 0, 1, ..., n \tag{4.2.4}$$

$$\text{où } B_i = \begin{pmatrix} b_{0,i} \\ b_{1,i} \\ b_{2,i} \\ \vdots \\ b_{n,i} \end{pmatrix} \text{ pour } i = 0, 1, ..., n$$

Soit la série formelle $\overline{y}(x) = \sum_{i=0}^{\infty} a_i x^i$; $\varphi(x)$ est les $(N+1)$ premiers termes de $\overline{y}(x)$, veut dire que :

$$\varphi(x) = a_0 + a_1 x + ... + a_N x_N$$

On va utiliser ce lemme dans notre algorithme.

Lemme 4.2.1 *:*

Soit $G(x,y)$ un polynôme irréductible, non trivial dans $\overline{\mathbb{Q}}[x,y]$, où $\deg(G,x) = m$, $\deg(G,y) = n$, et soit $\overline{y}(x)$ la série formelle qui vérifie $G(x,y) = 0$ et $\varphi(x)$ les $(2mn+1)$ premiers termes de $\overline{y}(x)$.

Si $Q_0(x), Q_1(x), ..., Q_n(x) \in \overline{\mathbb{Q}}[x]$ tels que $Q_0(x) + Q_1(x)\varphi(x) + ... + Q_n(x)\varphi^n(x) = 0(x^{2mn+1})$, où $\deg(,x) \leq m$ et les $Q_i(x)$ ne sont pas tous nuls, alors :

$$G(x,y) = \lambda(Q_0(x) + Q_1(x)y + ... + Q_n(x)y^n) \tag{4.2.5}$$

où $\lambda \in \overline{\mathbb{Q}}$ et non nul.

Preuve. : Soit $Q(x,y) = Q_0(x) + Q_1(x)y + ... + Q_n(x)y^n$, il existe S ,$T \in \overline{\mathbb{Q}}[x,y]$ tels que :

$$SG(x,y) + TQ(x,y) = Res_y(G,Q) \tag{4.2.6}$$

où : $\deg(S,y) < n$ et $\deg(T,y) < n$.

∘ Si $Q(x,\overline{y}(x)) = 0$ alors la relation (4.2.5) est vraie.

∘ Supposons que $Q(x,\overline{y}(x)) \neq 0$ et $Res_y(G,Q) \neq 0$ alors $\deg(Res_y(G,Q),x) \leq 2mn$ on remplace y par $\overline{y}(x)$ dans (4.2.6) , alors le membre à gauche sera :

$$SG(x,\overline{y}(x)) + TQ(x,\overline{y}(x)) = TQ(x,\overline{y}(x))$$

car $G(x,\overline{y}(x)) = 0$.

$$TQ(x,\overline{y}(x)) = T(Q_0(x) + Q_1(x)\overline{y}(x) + ... + Q_n(x)\overline{y}(x)^n)$$

On sait que $\overline{y}(x) = \sum_{i=0}^{\infty} a_i x^i$, alors le degré du membre gauche en x est d, tel que $d > 2mn$: d'où une contradiction, donc $Res_y(G,Q) = 0$ ce qui implique que :

$$G(x,y) = -\frac{T}{S}Q(x,y)$$

On sait que $G(x,y)$ est irréductible, alors $-\frac{T}{S} \in \overline{\mathbb{Q}}$, en posant $-\frac{T}{S} = \lambda$, on aura donc $G(x,y) = \lambda Q(x,y)$. ■

Algorithme 4.2.1 *:*

Premièrement, on donne un algorithme pour calculer les $N+1$ termes d'une série formelle solution de l'équation $F = 0$, pour un entier positif N.

Regardons $F = 0$ comme une courbe algébrique.

On détermine un point (z_0, z_1) tels que $F(z_0, z_1) = 0$ et $S(z_0, z_1) \neq 0$, puis on peut calculer les $y_i = z_i$ étape par étape et enfin $\overline{y}(x) = z_0 + z_1 x + \frac{z_2}{2!}x^2 + ...$ est une série formelle solution de l'équation $F = 0$.

L'algorithme est le suivant :

L'entrée : un polynôme différentiel irréductible $F(y)$ du premier ordre et un entier $N > 0$

la sortie : les $N+1$ termes d'une série formelle solution de $F = 0$.

1) Déterminer $(z_0, z_1) \in \overline{\mathbb{Q}}^2$ de $F(y, y_1) = 0$ tq $S(z_0, z_1) \neq 0$ et $z_1 \neq 0$.

2) $i := 2$ et $\varphi(x) := z_0 + z_1 x$

3) Quand $i \leq N$ faire

   (a) remplacer y par $\varphi(x)$ et y_1 par $\varphi'(x)$ dans $F(y, y_1)$.

   (b) $c :=$ le coefficient de x^{i-1} dans $.F(\varphi(x), \varphi'(x))$.

   (c) $z_i := -\frac{(i-1)!c}{S(z_0,z_1)}$ et $\varphi(x) := \varphi(x) + \frac{z_i}{i!}x^i$.

   (d) $i := i + 1$.

4- Retourner $(\varphi(x))$.

Soit $\overline{y}(x)$ la série formelle, solution de l'équation $F = 0$, alors d'aprés (2.1.1) , on a :

$$F(\overline{y}(x), \overline{y}_1(x))^{(i-1)} = S(\overline{y}(x), \overline{y}_1(x)).\overline{y}_i(x) + R\left(\overline{y}(x), ..., \overline{y}_{i-1}(x)\right) = 0$$

Comme $\overline{y}_k(x)\,|_{x=0} = z_k$ pour $k = 1, 2, ...$, on a donc :

$$S(z_0, z_1).z_i + R(z_0, ..., z_{i-1}) = 0$$

ce qui implique que

$$z_i = -\frac{R(z_0, ..., z_{i-1})}{S(z_0, z_1)}$$

D'autre part, supposons que $\varphi(x) = z_0 + z_1 x + ... + \frac{z_{i-1}}{(i-1)!} x^{i-1}$.
On a donc $\varphi^{(i)}(x) = 0$ et la relation (2.1.1) sera :

$$F(\varphi(x), \varphi'(x))^{(i-1)} = R\left(\varphi(x), ..., \varphi^{(i-1)}(x)\right)$$

comme $\varphi^{(k)}(x)(x) \mid_{x=0} = z_k$ pour $k = 1, 2, ..., i-1$, on a donc :

$$F(\varphi(x), \varphi'(x))^{(i-1)} \mid_{x=0} = R(z_0, ..., z_{i-1})$$

comme $F(\varphi(x), \varphi'(x))^{(i-1)} \mid_{x=0} = (i-1)!c$, alors : $z_i = -\frac{(i-1)!c}{S(z_0, z_1)}$

Algorithme 4.2.2 *:*

L'entré : un polynôme différentiel irréductible $F(y)$ du premier ordre.
La sortie : une solution algébrique de $F = 0$, si elle existe

1- $d := \deg(F, y_1)$ et $e := \deg(F, y)$

2- $k := 1$

Tant que $k \leq d + e$ faire

(a) Calculer les premiers $2dk + 1$ termes $\varphi(x)$ d'une série formelle solution de $F = 0$, d'aprés l'algorithme (4.2.1)

(b) $a_i :=$ le coefficient de x^i dans $\varphi(x)$ pour $i = 0, ..., 2dk$.

(c) Dans (4.2.2) et (4.2.3) poser $m = d, n = k$ et $N = 2dk$.
on construit les équations linéaires (4.2.4) .

(d) Si (4.2.4) n'a pas de solution différente de zéro, ou la dimension de l'espace des solutions de (4.2.4) est plus grand que 1, passer donc à (i).

(e) Sinon, choisissez l'une des solutions non nulles $b_{i,j}$ où $i = 0, ..., d$ et $j = 0, ..., k$.

(f) $G(x, y) := \sum_{j=0}^{k} \sum_{i=0}^{d} b_{ij}\, x^i\, y^j$, $S = \frac{\partial G}{\partial y}$; $I :=$l'initial de $G(x, y)$.

(g) Si $\gcd(G, S) \neq 1$ ou $\gcd(G, I) \neq 1$ alors passez à l'étape (i). Sinon, passez à l'étape suivante.

(h) Soit $R = prem(F, G)$. Si $R = 0$, alors retourner $G(x, y) = 0$.

(i) $k := k + 1$.

La complexité des algorithmes précédents dépend entièrement de la complexité de l'algorithme de paramétrisation. Finalement on donne l'exemple suivant .

Exemple 4.2.1 *:*

Soit $(y^6+2y+1)y'^3-(12y^5+9y^4-1)y'^2+27y^8+54y^7+27y^6+4y^3 = 0$

On considère $F = (y^6 + 2y + 1)y_1^3 - (12y^5 + 9y^4 - 1)y_1^2 + 27y^8 + 54y^7 + 27y^6 + 4y^3$

Alors on a :

1. $d = 3$ et $e = 8$.

2. $(1; -2)$ est un point de $F(y; y_1) = 0$ qui satisfait l'hypothèse de l'étape 1 de l'algorithme .(4.2.1)

3. Pour le cas $k = 1$, on obtient un $G(x, y) = 0$ qui n'est pas la solution de $F = 0$.

Nous donnons ici seulement le processus dans le cas $k = 2$.

4. Les 13 premiers termes de la série formelle solution de $F = 0$ sont :

$\varphi(x) = 1-2x+\frac{5}{2}x^2-\frac{9}{4}x^3+\frac{1}{2}x^4+\frac{5}{4}x^5-\frac{41}{32}x^6-\frac{65}{64}x^7+\frac{363}{128}x^8-\frac{111}{256}x^9-\frac{2545}{512}x^{10}+\frac{5141}{1024}x^{11}+\frac{5891}{2048}x^{12}$

5. Soient $m = 3$, $n = 2$ et $N = 12$, on construit les équations linéaires (4.2.4) par résolution, nous obtenons une solution différente de zéro : $(-1; 1; 0; 0; 0; 3; -3; 1; 1; 0; 0; 0)$

6. $G(x; y) = -1 + x + 3xy - 3x^2y + x^3y + y^2$.

7. $prem(F, G) = 0$, donc $G(x; y) = -1 + x + 3xy - 3x^2y + x^3y + y^2 = 0$ est une solution algébrique de $F = 0$.

Dans ce mémoire , nous donnons une condition necéssaire et suffisante pour qu'une équation différentielle ordinaire posséde une solution générale algébrique. Pour une équation différentielle du premier ordre, nous donnons la structure et le degré de sa solution générale algébrique, et un algorithme pour le calcul de cette solution si elle existe. L'algorithme est basé sur la paramètrisation des courbes algébriques planes, et l'approximation algébrique, qui est un type spécial de l'approximation de Padé-Hermite.

Bibliographie

[1] Lang, S; Introduction to Algebraic and Abelian Fonctions, second edition, Springer-Verlag, New york, 1972.

[2] Kolchin, E . R; Differential Algebra and Algebraic groups, Academic Press, New york, 1950.

[3] Ritt, JF; Differential Algebra. Amer. Math. Sco. Colluquim, New york, 1950.

[4] Kovacic, J, J; An algorithm for solving second ordre Linear Homogeneous Differential equations, J. Symb. comput 2 (1), 3- 43, 1986.

[5] Davenport, J. H, On the integration of Algebraic Fonctions, Lecture notes in computer science Springer-Verlag, New york, 1981.

[6] Irving Kaplansky; An introduction to Differential Algebra, Hermann, Paris,1957.

[7] Fulton William, Algebraic curves. Addison-Wesley Publishing company, Inc, University of Chicago.

[8] Robert J. Walker, Algebraic curves, Princeton Unv. Press, 1950.

[9] Michael. F. Singer; Liouvillian solutions of Linear Differential equations with Liouvillian coefficients, J. Symb. Comput 11, 251-273, 1991.

[10] Feng R, and Gao X,S, Rational general solutions of algebraic ordinary differential equations, proc. Issac 2004, 155-162, ACM Press, 2004.

[11] Trager, B, Integration of Algebraic Fonctions, Ph. D thesis, Dpt of EECS, Massachusetts instute of technology, 1984.

[12] Herz. J. C, Ideaux differentiels, Seminaire Dubreil, Dpt d'algèbre et théorie des nombres, Paris, tome 5-6, p 1-10, 1951-1953.

[13] J. M. Aroca and J. Cano, R . Feng and X. S. Gao Algebraic general solutions of algebraic ordinary differential equations, proc. Issac 2005, 24-27, ACM Press, 2005.

[14] Rish, R . H; the problem of integration in finite terms, Trans AMS, 139, 167-189, 1969.

[15] D, Behloul; Polynomial solutions of a generalization of the first Painlevé differential equation, App. Math. E-Notes, 148-158, Vol 11, 2011.