**République Algérienne Démocratique et Populaire**

*Ministère de l'Enseignement Supérieur et de la Recherche Scientifique*

**Université Mohamed Seddik Ben Yahia-Jijel**

**Faculté des Sciences Exactes et informatique**

**Département de Mathématiques**

*Mémoire*

***Pour l'obtention du diplôme de Master***

***Spécialité :*** *Mathématiques*

***Option :*** *Mathématiques fondamentales*

***Thème :***

# Extensions de Liouville

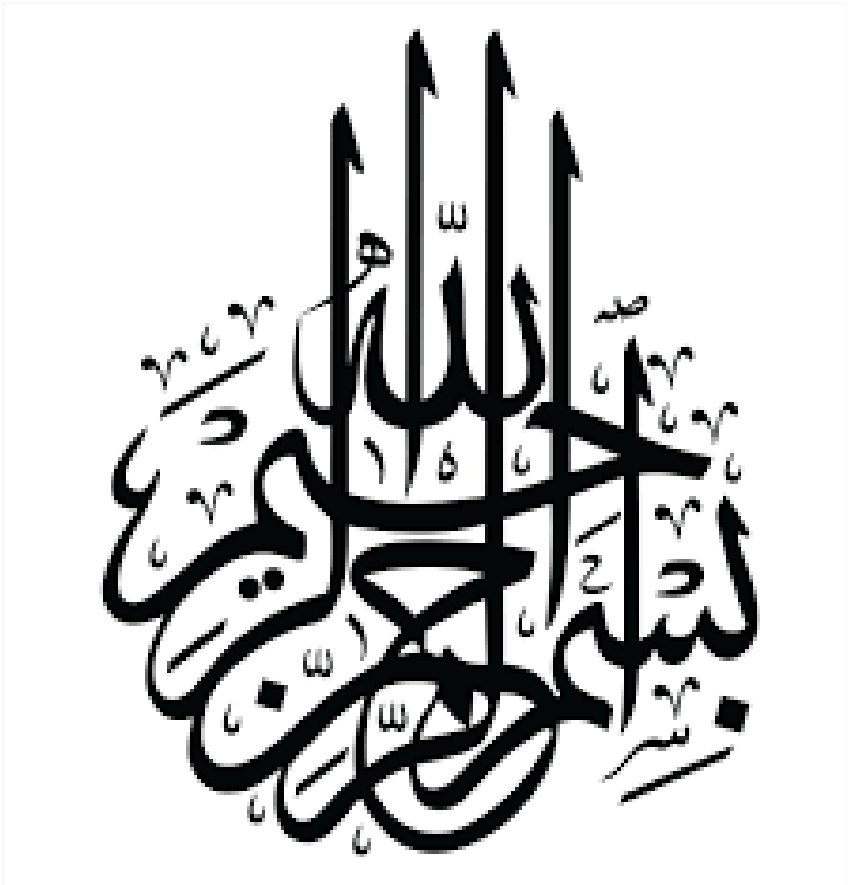
Présenté par

**Saida Boualbani**

Soutenu devant les membres du jury

| | | | |
|---|---|---|---|
| **Président :** | **N. Touafek** | **Pref** | **Univ. De Jijel** |
| **Encadreur :** | **M. Kemiha** | **M.A.A** | **Univ. De Jijel** |
| **Examinateur :** | **A. Bouchair** | **M.C.A** | **Univ. De Jijel** |

**Promotion : 2016/2017**


بسم الله الرحمن الرحيم

# *Remerciements*

*Mes remerciements vont particulièrement à mon DIEU, pour m'avoir accordé ce travail et m'avoir donné la force pour le mener à terme.*

*Je tiens en premier temps à remercier*

***Mme Mounira Kemiha***

*pour m'avoir confié ce travail ainsi que pour son aide, ses précieux conseils, sa patience et sa disponibilité.*

*Je remercie les membres de jury*

***Mr. Nouressadat Touafek***

*et*

***Mr Abd rahmane Bouchair***

*d'avoir bien voulu accepter de juger ce travail.*

*Ainsi une grande salutation à mes chers parents pour leurs dévouements, leur amour et leurs encouragements durant toutes les années d'étude.*

*Et à la fin je souhaite adresser mes sincères remerciements à tous mes amis et mes camarades.*

# DEDICACES

*D'abord je dédie ce travail à mes très chers parents,*
*qui m'ont encouragés et me aider et éclairés le chemin et en me donnant tous jours la main,*
*je dis à mon Dieu garde les.*

*Et bien sûr à mes frères*
*A mes sœurs à petite cher Salsabil*

*A mes chères amies les étudiants de Master II Mathématiques Fondamentales.*
*Aux enseignants qui ont contribué à ma formation.*

# Table des matières

# Introduction

La théorie de Galois classique est apparue àfin de déterminer les équations polynomiales résolubles par radicaux, l'idée centrale de cette théorie est d'associer à une telle équation son groupe de Galois qui est le groupe d'automorphismes de son corps de décomposition .

La résolubilité par radicaux de l'équation $P(X) = 0$ où $P$ est un polynôme irréductible est alors liée à la résolubilité de ce groupe.

Une théorie analogue adaptée aux équations différentielles linéaires à été développée des la fin de $XIX^{\text{ième}}$ ciecle notament par Picard-Vessiot introduisant le groupe de Galois différentiel associé à de telles équations.

L'étude de ce dernier permet de caractériser ces solutions. Une solution est dite liouvillienne ou de Liouville si elle est élément d'une extension de Liouville elle est obtenue à partir des coefficients de l'équation uniquement, à l'aide d'un nombre fini d'intégrations, d'exponentielles et de résolution d'équations algébriques. Cette appellation est adoptée en homage à Liouville l'un de ceux qui contribuèrent à sortir les travaux de Galois de l'oubli, il lui renvient le mérite d'avoir découvert le critère de résolubilité de ces équations par les opérations élémentaires déjà citées.

L'existence de solutions Liouvilliennes et donc d'extensions de Liouville est liée fortement à l'étude du groupe de Galois différentiel associé à ce genre d'équations c'est ce qui fera l'objet de ce travail.

Ce dernier est constitué de trois chapitres, dans le premier chapitre on trouve des notions de base concernant les groupes résolubles, les anneaux les extensions de corps et quelques éléments de la topologie de Zariski.

La deuxième chapitre est une introduction à la théorie de Galois différentielle où on trouve des notions concernant les corps associées à un système différentiel linéaire d'ordre un et on termine par les propriétés du groupe de Galois différentiel.

Le troisième chapitre est consacré essentiellement aux extensions de Liouville. L'existence de ces extensions est lieé fortement à la résolubilité du groupe de Galois associé.

Pour plus de détails sur cette théorie qui passe même en caractéristique positive, aux équations nonlinéaires ainsi qu'aux equations aux différences et en théorie des nombres on peut se référer à [1],[8],[9], [10],[12],[14] et [15].

# Chapitre 1

# Résultats Préliminaires

Ce chapitre est consacré essentielement aux notions de bases sur les groupes résolubles, les anneaux et les extension de corps.

## 1.1 Définitions et Premières Propriétés

### 1.1.1 Groupes résolubles

**Définition 1.1.1**
*Soit $(G, .)$ un groupe. Un sous groupe $H$ de $G$ est dit normal dans $G$ et on note $H \lhd G$ si on a : $\forall a \in G : aHa^{-1} = H$.*

**Définition 1.1.2**
*Soit $S$ une partie non vide de $G$, on appelle sous groupe engendré par $S$ et on note $< S >$ l'ensemble $\{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} / n \in \mathbb{N}^*, x_i \in S,\ \alpha_i = \pm 1;\ 1 \leq i \leq n\}$, c'est le plus petit sous groupe de $G$ contenant $S$.*

**Définition 1.1.3**
*Soient $x, y$ deux éléments dans $G$, on appelle commutateur de $x$ et $y$ l'élément $xyx^{-1}y^{-1}$ qu'on note $[x, y]$.*

**Lemme 1.1.1**
*Soient $x, y, z \in G$. Alors on a :*

$$[x, y]^{-1} = [y, x] \qquad , \qquad z[x, y]z^{-1} = [zxz^{-1,}, zyz^{-1}].$$

**Démonstration.**

$[x,y]^{-1} = (xyx^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1}y^{-1}x^{-1}$

$$= yxy^{-1}x^{-1} = [y,x].$$

et

$z[x,y]z^{-1} = z[xyx^{-1}y^{-1}]z^{-1} = zxz^{-1}.zyz^{-1}.zx^{-1}z^{-1}.zy^{-1}z^{-1}$

$$= (zxz^{-1})(zyz^{-1})(zxz^{-1})^{-1}(zyz^{-1})^{-1}$$

$$= [zxz^{-1}, zyz^{-1}].$$

■

**Définition 1.1.4**

*Le sous groupe de $G$ engendré par la partie $S = \{xyx^{-1}y^{-1}/x, y \in G\}$ est appelé le groupe des commutateurs ou le groupe derivé de $G$ et est noté $G'$.*

**Exemple 1.1.1**

*Soit $G = GL_2(\mathbb{R})$ le groupe des matrice inversibles à coefficients réels.*
*Tout élément de $G'$ est le produit des $[A,B]$ ou $A, B \in GL_2(\mathbb{R})$, on a $[A,B] = A^{-1}B^{-1}AB$ donc :*

$$\begin{aligned} det([A,B]) &= det(A^{-1}B^{-1}AB) \\ &= det(A^{-1}).det(B^{-1}).det(A).det(B) \\ &= \frac{1}{det(A)}\frac{1}{det(B)}.det(A).det(B) = 1. \end{aligned}$$

*donc $G' \subset \{A \in GL_2(\mathbb{R});\ det(A) = 1\} = SL_2(\mathbb{R})$.*
*Il nous faut maintenant considérer l'inclusion inverse. Notons premièrement que nous avons la factorisation (décomposition de Iwasawa [4]) :*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{a}{\sqrt{a^2+c^2}} & \frac{-c}{\sqrt{a^2+c^2}} \\ \frac{c}{\sqrt{a^2+c^2}} & \frac{a}{\sqrt{a^2+c^2}} \end{pmatrix} . \begin{pmatrix} \sqrt{a^2+c^2} & 0 \\ 0 & \frac{1}{\sqrt{a^2+c^2}} \end{pmatrix} . \begin{pmatrix} 1 & \frac{(ab+cd)}{(a^2+c^2)} \\ 0 & 1 \end{pmatrix}$$

*Si $ad - bc = 1$. Cette expression est obtenue en considérant les colonnes de $M$ comme des vecteurs de $\mathbb{R}^2$ et en utilisant l'algorithme de Gram-Schmidt nous pouvons déterminer une base*

*orthonormale. Celle-ci nous donne les colonnes de la première matrice dans la factorisation. Nous pouvons remarquer que*

$$\begin{pmatrix} \frac{a}{\sqrt{a^2+c^2}} & \frac{-c}{\sqrt{a^2+c^2}} \\ \frac{c}{\sqrt{a^2+c^2}} & \frac{a}{\sqrt{a^2+c^2}} \end{pmatrix} = \begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix} \qquad pour \theta \in [0, 2\pi[;$$

$$\begin{pmatrix} \sqrt{a^2+c^2} & 0 \\ 0 & \frac{1}{\sqrt{a^2+c^2}} \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \qquad pour \alpha \in \mathbb{R}_+^*;$$

$$\begin{pmatrix} 1 & \frac{ab+cd}{a^2+c^2} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \qquad pour \beta \in \mathbb{R}.$$

*Ce qui précéde montre que $SL_2(\mathbb{R})$ par l'ensemble des matrices*

$$\begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$$

*Où $\theta \in [0, 2\pi[, \alpha \in \mathbb{R}_+^*$ et $\beta \in \mathbb{R}$. Il nous suffit donc de montrer chacune de matrices peut s'écrire comme un commutateur d'éléments de $GL_2(\mathbb{R})$. On a :*

$$\begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix} = \begin{pmatrix} cos(\theta/2) & sin(\theta/2) \\ -sin(\theta/2) & cos(\theta/2) \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \cdot$$

$$\begin{pmatrix} cos(\theta/2) & sin(\theta/2) \\ -sin(\theta/2) & cos(\theta/2) \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

$$\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

*De tout ceci, nous obtenons que $SL_2(\mathbb{R}) \subset G'$. Donc $SL_2(\mathbb{R}) = (GL_2(\mathbb{R}))'$.*

**Proposition 1.1.2**

*Soient $G$ un groupe et $G'$ le groupe des commutateurs . On a alors :*

(1) *$G'$ est le plus petit sous-groupe normal de $G$.*

(2) *Le groupe quotient $G/G'$ est commutatif.*

(3) *$G$ est commutatif si et seulement si $G' = \{e\}$.*

**Définition 1.1.5**

*On dit que $G$ est résoluble s'il existe une chaine de sous groupes*
*$G_0 = G \supseteq G_1 \supseteq ... \supseteq G_m = \{e\}$ tel que $\forall i = \overline{1,m}$, $G_{i+1}$ normal dans $G_i$ et $G_i/G_{i+1}$ commutatif.*

**Définition 1.1.6**

*On appelle série dérivée de $G$ la série $G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq ...$ où $G^{(0)} = G$ et $G^{(i+1)} = (G^{(i)})'$*
*La longueur de la série dérivée de $G$ est le plus petit entier $m$ tel que $G^{(m)} = \{e\}$*

**Théorème 1.1.3**

*$G$ est résoluble si et seulement si la série dérivée de $G$ a une longeur finie*

**Proposition 1.1.4**

*Le sous groupe d'un groupe résoluble est résoluble et l'image d'un groupe résoluble par un homomorphisme de groupes est un groupe résoluble*

### 1.1.2 Anneaux et Corps

Soit $A$ un anneau commutatif d'éléments neutres 0 et 1.

**Définition 1.1.7**

*La caractéristique de l'anneau $A$ est le plus petit entier $n \in \mathbb{N}$ verifiant $n.1 = 0$ où*
*$n.1 = 1 + 1 + \ldots + 1$.*

**Lemme 1.1.5**

*La caractéristique d'un corps est soit nulle, soit égale à un nombre premier.*

**Exemple 1.1.2**

– *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0.*
– *$\mathbb{Z}/n\mathbb{Z}$ de caractéristique $n$.*

**Définition 1.1.8**

*Un élément $x \in A$ est inversible s'il existe $y \in A$ tel que $xy = yx = 1$. Les éléments inversibles de $A$ forment un groupe appellé le groupe des unités de $A$ noté $U(A)$.*

**Définition 1.1.9**

*Un élément $x$ dans $A$ est dit premier si $x \neq 0$ et $x \notin U(A)$ et si pour tout produit $a.b$ divisible par $x$, l'un des deux facteurs $a$ ou $b$ est divisible par $x$.*

**Définition 1.1.10**

*Un élément $x$ dans $A$ est dit irréductible si $x \neq 0$ et $x \notin U(A)$ et si pour tout $a, b \in A$ :*
$x = a.b \Longrightarrow a \in U(A) \vee b \in U(A)$

**Lemme 1.1.6**

*Si $A$ est intègre, on a : $x$ est premier $\Longrightarrow$ $x$ est irréductible.*

**Démonstration.**

Supposons que $x$ est premier donc $x \neq 0$ et $x \notin U(A)$.
Soint $a, b \in A$ tels que : $\quad x = a.b \ldots (*)$

$(*) \quad \Longrightarrow$ ($x$ divise $a$) $\vee$ ($x$ divise $b$)

$\Longrightarrow (\exists a' \in A \ ; \ a = x.a') \vee (\exists b' \in A \ ; \ b = x.b')$

$\Longrightarrow (\exists a' \in A \ ; \ x = x.a'b) \vee (\exists b' \in A \ ; \ x = ax.b')$

$\Longrightarrow (\exists a' \in A \ ; \ x(1 - a'b) = 0) \vee (\exists b' \in A \ ; \ x(1 - ab') = 0)$

$\Longrightarrow ((1 - a'b) = 0) \vee ((1 - ab') = 0)$

$\Longrightarrow b \in U(A) \vee a \in U(A)$.

■

**Définition 1.1.11**

*Un idéal d'un anneau commutatif $A$ est un sous ensemble $I \subset A$ tel que :*
*(i) $I$ est un sous groupe de $(A, +)$*
*(ii) $\forall x \in I, a \in A : ax \in I$ .*

**Proposition 1.1.7**

*Soit $I$ un idéal de $A$ ; on a : $I = A \Longleftrightarrow \exists \, x \in I \ / x \in U(A)$.*

**Proposition 1.1.8**

*$A$ est un corps $\Longleftrightarrow$ les seuls idéaux de $A$ sont $\{0\}$ et $A$.*

**Lemme 1.1.9**

*Si $I$ un idéal de $A$ alors :*
*$\sqrt{I} = \{a \in A; \exists n \in \mathbb{N}^*, a^n \in I\}$ est un idéal de $A$, appelé l'idéal radical de $I$.*

**Définition 1.1.12**

*Un élément $x \in A$ est dit nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$. L'ensemble des éléments nilpotents de $A$ est l'idéal $\sqrt{\{0\}}$.*

**Définition 1.1.13**

*Pour tout $x \in A$, l'ensemble $xA = \{xa : a \in A\}$ est un idéal de $A$, appelé l'idéal principal engendré par $x$.*

**Définition 1.1.14**

*L'anneau commutatif $A$ est dit principal si $A$ est intégre et si tout idéal de $A$ est un idéal principal.*

**Exemple 1.1.3**

*Si $K$ est un corps commutatif, $K[X]$ est un anneau principal.*
*En effet : soit $I$ un idéal de $K[X]$ et $P \in I$ non nul de dégré minimum*
*On a $P \in I$ donc $< P > \subset I$.*
*Soit $Q \in I$, par division euclidienne on a, $Q = SP + R$ avec $d^\circ(R) < d^\circ(P)$ ou $R = 0$.*
*Si $d^\circ(R) < d^\circ(P)$, comme $R = Q - SP \in I$ ceci mene à une contradiction, donc $R = 0$ et donc $Q = PS \in < P >$ et $I = < P >$ .*

**Définition 1.1.15**

*Un idéal $P$ de $A$ est dit premier si :*
*(i)* $P \neq A$
*(ii)* $\forall x, y \in A : x.y \in P \Longrightarrow x \in P \vee y \in P$.

**Définition 1.1.16**

*Un idéal $M$ de $A$ est dit maximal si :*
*(i)* $M \neq A$
*(ii) pour tout idéal $J \subset A : M \subset J \Longrightarrow J = A \vee J = M$.*

**Exemple 1.1.4**

*L'idéal $I = \{f \in \mathcal{C}(\mathbb{R}, \mathbb{R}); f(0) = 0\}$ de $\mathcal{C}(\mathbb{R}, \mathbb{R})$ est un idéal maximal .*
*En effet : soit $J$ idéal de $\mathcal{C}(\mathbb{R}, \mathbb{R})$ tel que $I \subsetneq J$.*
*Soit $g \in J - I$ donc $g(0) \neq 0$ on a la fonction $g - g(0)$ s'annule en 0 donc $g - g(0) \in I \subsetneq J$*
*on a aussi $g(0) = g - (g - g(0) \in J$ et $g(0)$ est inversible dans $\mathcal{C}(\mathbb{R}, \mathbb{R})$*
*donc $J = \mathcal{C}(\mathbb{R}, \mathbb{R})$*

**Définition 1.1.17**

*Soit $A$ et $B$ deux anneaux, on appelle morphisme d'anneaux toute application $f : A \longrightarrow B$ vérifiant :*

- $f(x+y) = f(x) + f(y)$, $\forall x, y \in A$.
- $f(xy) = f(x)f(y)$, $\forall x, y \in A$.
- $f(1_A) = 1_B$.

**Remarque 1.1.1**

*Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Le noyau de $f$, $ker(f) = \{a \in A, f(a) = 0\}$ est un idéal de $A$.*

**Remarque 1.1.2**

*Si $A, B$ sont des corps et si $f : A \longrightarrow B$ est un morphisme d'anneaux, alors $f$ est injectif.*
*En effet : on a $f(1_A) = 1_B$ donc $f \neq 0 \Longrightarrow ker(f) \neq A \Longrightarrow ker(f) = \{0\}$ car $A$ est un corps.*

**Théorème 1.1.10**

*Pour tout idéal $I$ de $A$, le quotient $A/I$ est un anneau commutatif, et la surjection canonique $\pi : A \longrightarrow A/I$ est un morphisme d'anneaux .*

**Proposition 1.1.11**

*Soit $I$ un idéal de $A$ :*
(1) *$I$ est premier $\Longleftrightarrow$ $A/I$ est un anneau intégre.*
(2) *$I$ est maximal $\Longleftrightarrow$ $A/I$ est un corps.*

**Définition 1.1.18**

*On dit qu'un anneau $A$ est noethérien si tout idéal de $A$ est engendré par un nombre fini d'éléments.*

**Théorème 1.1.12**

*Tout anneau principal est noethérien.*

**Proposition 1.1.13**

*$A$ est noethérien $\Longleftrightarrow$ toute suite croissante d'ideaux $I_0 \subseteq \ldots \subseteq I_n \subseteq \ldots$ est stationnaire .*

**Exemple 1.1.5**

*Si $K$ est un corps, alors $K[X_1, \ldots, X_n]$ est noethérien.*

### 1.1.3 Produit tensoriel

**Théorème 1.1.14**

*Soient $E$ et $F$ deux espaces vectoriels sur un corps commutatif $K$.*
*Il existe un $K$-espace vectoriel, noté $E \otimes F$, et une application bilinéaire*

$$\varphi : E \times F \longrightarrow E \otimes F;\ \varphi(x, y) \longmapsto x \otimes y$$

*et pour toute application bilinéaire $\psi : E \times F \longrightarrow F$, il existe une et une seule application linéaire $f : E \otimes F \longrightarrow F$ telle que : $\psi = f \circ \varphi$.*
*Le espace $E \otimes F$ est unique à isomorphisme près.*

**Définition 1.1.19**

*Le $K$-espace vectoriel $E \otimes F$ est appelé le produit tensoriel de $E$ et $F$, et $x \otimes y$ appelé le produit tensoriel de $x$ et $y$.*

**Proposition 1.1.15**

*Si $E$ et $F$ sont de dimension finie $n$, $m$ respectivement , alors :*

$$dim(E \otimes F) = dim(E) \times dim(F) = nm$$

*et Si $\{e_i;\ 1 \leq i \leq n\}$ et $\{f_j;\ 1 \leq j \leq m\}$ sont respectivement des bases de $E$ et $F$, alors $\{e_i \otimes f_j;\ 1 \leq i \leq n,\ 1 \leq j \leq m\}$ est une base de $E \otimes F$.*

### 1.1.4 K-Algèbres

**Définition 1.1.20**

*Soient $K$ un corps commutatif et $E$ un ensemble muni de deux lois internes $+$ et $\times$, et une loi externe $(.)$ sur $K$ Alors $(E, +, \times, .)$ est une $K$-algèbre ssi :*
•*$(E, +, .)$ est un $K$-espase vectoriel.*
• *La loi $\times$ est distributive sur $+$ :*
$(x + y) \times z = x \times z + y \times z;\ \forall x, y, z \in E.$
• *La loi $\times$ est associative :*
$(x \times y) \times z = x \times (y \times z); \forall x, y, z \in E$
• $(\lambda.x) \times y = x \times (\lambda.y) = \lambda.(x \times y);\ \forall x, y \in E;\ \forall \lambda \in K$

**Définition 1.1.21**

*Une $K$-algèbre $E$ est dite de type fini s'il existe un nombre fini d'éléments $x_1, \ldots, x_n$ de $E$ tels que : $E = K[x_1, \ldots, x_n]$.*

**Proposition 1.1.16**

• *Tout quotient d'une $K$-algèbre de type fini par un idéal est une $K$-algèbre de type fini.*

• *Pour toute $K$-algèbre de type fini $E_1$ et $E_2$, le produit tensoriel $E_1 \otimes_K E_2$ est une $K$-algèbre de type fini.*

### 1.1.5 Topologie de Zariski

Soit $K$ un corps commutatif.

**Définition 1.1.22**

*Soit $K[X_1, \ldots, X_n]$ l'anneau des polynomes à n indeterminées $X_1, \ldots, X_n$ et soit $P \in K[X_1, \ldots, X_n]$. La fonction $P : K^n \longrightarrow K$ ; $(x_1, \ldots, x_n) \longmapsto P(x_1, \ldots, x_n)$ est appelée la fonction polynomiale associée à $P$.*

**Définition 1.1.23**

*Soit $J$ une famille de fonctions polynomiales définies sur $K^n$.*
*L'ensemble $V(J) = \{x \in K^n; P(x) = 0; P \in J\}$ est appelé l'ensemble des zéros de $J$.*

**Proposition 1.1.17**

*Soient $J_1, J_2$ deux familles de fonctions polynomiales .*
*1− si $J_1 \subset J_2$ alors $V(J_2) \subset V(J_1)$.*
*$2 - V(J_1) \cup V(J_2) = V(J_1.J_2)$ et $\cap_i V(J_i) = V(\cup_i J_i)$*

**Définition 1.1.24**

*Siot $U \subset K^n$, $U$ est dit algébrique s'il existe une famille de fonctions polynomiales $J$ telle que : $U = V(J)$.*

**Exemple 1.1.6**

1) $\emptyset = V(\{1\}), \qquad K^n = V(\{0\})$.
2) *Soit* $J = \{X^4 - 2\}$.
*Si* $K = \mathbb{C}$, $V(J) = \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$.
*Si* $K = \mathbb{R}$, $V(J) = \{\pm\sqrt[4]{2}\}$.
*Si* $K = \mathbb{Q}$, $V(J) = \emptyset$.

**Proposition 1.1.18**

*Soient $U_1, U_2$ deux ensembles algébriques de $K^n$. On a $\cap_i U_i$ et $U_1 \cup U_2$ sont algébriques.*

**Démonstration.**

$(U_i)_{i\in I}$ algébriques $\Longrightarrow \exists\ (J_i)_{i\in I}$ familles de fonctions telles que $U_i = V(J_i)$

D'apré la proposition 1.1.17 : $\cap_i V(J_i) = V(\cup_i J_i)$

$U_1, U_2$ algébriques $\Longrightarrow \exists\ J_1, J_2$ deux familles de fonctions telles que $U_1 = V(J_1)$ et $U_2 = V(J_2)$.

D'apré la proposition 1.1.17 : $U_1 \cup U_2 = V(J_1) \cup V(J_2) = V(J_1.J_2)$. ■

**Définition 1.1.25**

*On appelle Topologie de Zariski $\tau$ sur $K^n$ la topologie qui prend comme fermés les sous-ensembles algébriques de $K^n$, qu'on appelle aussi fermés de Zariski.*

*Les ouverts pour cette topologie sont les complémentaires des fermés.*

**Proposition 1.1.19**

*Pour toute suite décroissante de fermés $X_0 \supset X_1 \supset \ldots \supset X_n \supset \ldots$, il existe $k_0 \in \mathbb{N}$ tel que $X_i = X_{k_0}$, $\forall i \geq k_0$. On dit que la suite $X_0 \supset X_1 \supset \ldots \supset X_n \supset \ldots$, est stationnaire*

**Démonstration.**

$K[X_1, \ldots, X_n]$ est noethérien, $I(X_i)$ est stationnaire donc $(X_i)_i$ est stationnaire, $I(X_i)$ designe l'idéal de $K[X_1, \ldots, X_n]$ défini par : $I(X_i) = \{P \in K[X_1, \ldots, X_n] \ / \ P(x) = 0 \ \forall\ x \in X_i\}$. ■

**Définition 1.1.26**

*Soit $F$ un fermé de Zariski. On dit qu'il est irrèductible s'il n'est pas réunion de deux fermés de Zariski.*

**Exemple 1.1.7**

*Soit $P(x, y) = x^2 - y^2$. Alors $V(\{P\}) = V(\{x - y\}) \cup V(\{x + y\})$, donc $V(\{P\})$ n'est pas irrèductible.*

**Proposition 1.1.20**

*Soit $F \in K^n$ un fermé de Zariski.*

$$F \text{ est irrèductible} \Longleftrightarrow \text{l'idéal } I(F) \text{ est premier.}$$

**Définition 1.1.27**

*Soit $(T, \tau)$ un espace topologique. La composante irrèductible est la plus grande partie irrèductible de $T$.*

**Définition 1.1.28**

*Soit $G$ un sous groupe de $GL(n, K)$, on dit que $G$ est un groupe algébrique si $G$ est un sous-ensemble fermé pour la topologie de Zariski de $GL(n, K)$.*

**Définition 1.1.29**

*Soit $G$ un groupe algèbrique, et soit $Id$ la matrice identité de $G$. On appelle composante connexe de l'identité de $G$ et on note $G^0$ la composante irrèductible de $G$ qui contient $Id$.*

**Proposition 1.1.21**

*Pour tout groupe algébrique $G$, il existe une seule composante connexe de l'identité de $G$.*

**Lemme 1.1.22**

*Soient $A, B \in GL(n,K)$. Les applications de $GL(n,K)$ dans $GL(n,K)$ ; $A \longmapsto A^{-1}$, $A \longmapsto A.B$, $A \longmapsto B.A$, $A \longmapsto A.B.A^{-1}$ et $A \longmapsto B.A.B^{-1}$ sont des applications algébriques, donc elles sont continues, et leurs inverses sont continues, elles sont donc des homéomorphismes.*

**Lemme 1.1.23**

*La composante connexe de l'identité $G^0$ d'un groupe algébrique $G$ est un sous-groupe algébrique, normal dans $G$, et l'indice $[G : G^0]$ de $G^0$ dans $G$ est fini. Les composantes connexes de $G$ sont les classes $G/G^0$.*

**Démonstration.**

L'image de $G^0$ par l'homéomorphisme $A \longmapsto A^{-1}$ de $G$ est une composante irrèductible de $G$ qui contient l'identité, donc $(G^0)^{-1} = G^0$. Soit $B \in G^0$, l'image de $G^0$ par l'homéomorphisme $A \longmapsto A.B$ est une composante irrèductible de $G$ qui contient l'identité, donc $G^0.G^0 = G^0$, alors $G^0$ est un sous-groupe de $G$.

Le groupe $G^0$ est fermé pour la topologie de Zariski, car c'est une composante irrèductible, donc $G^0$ est un sous-groupe linéaire algèbrique.

Soit $B \in G$, l'image de $G^0$ par l'homéomorphisme $A \longmapsto A.B.A^{-1}$ est aussi irréductible, donc $G^0 = B.G^0.B^{-1}$, donc $G^0$ normal dans $G$.

L'image de $G^0$ par l'homéomorphisme $A \longmapsto B.A$, est une composante irrèductible de $G$. Puisque le nombre des composantes connexes de $G$ est fini, l'indice de $G^0$ dans $G$ est fini.

L'ensemble $B.G^0$ est une composante irrèductible de $G$. Alors les composantes irrèductibles de $G$ sont les classes $G/G^0$. ∎

**Lemme 1.1.24**

*Soit $H$ un sous- groupe algébrique d'un groupe algébrique $G$ tel que le nombre de classes à droite de $G/H$ fini. Alors $H = G$.*

## 1.2 Extensions

### 1.2.1 Extension de corps

**Définition 1.2.1**

*Soit $K$ un corps. On appelle extension du corps $K$, toute paire $(L, \varphi)$ où $L$ est un corps et $\varphi : K \longrightarrow L$ un morphisme de corps, cette extension est notée $K \subset L$.*

**Remarque 1.2.1**

*Le morphisme $\varphi$ est injectif et permet d'identifier $K$ à un sous-corps de $L$ et $L$ a une structure de $K$-espace vectoriel; La dimension de $L$ sur $K$ si elle est finie est notée $dim_K(L)$.*

**Définition 1.2.2**

*Soit $K \subset L$. une extension de corps.*
*On appelle degré de l'extension $K \subset L$. la dimension $dim_K(L)$. On note ce nombre $[K : L]$, si $[K : L] < +\infty$, on dit que $K \subset L$ est de degré fini sur $K$.*

**Proposition 1.2.1**

*Soient $M$ un corps, $L$ un sous-corps de $M$, $K$ un sous-corps de $L$. Alors si $\{k_1, \ldots, k_n\}$ est une base de $L$ sur $K$ et $\{l_1, \ldots, l_m\}$ est une base de $M$ sur $L$, la famille $\{(k_i l_j) : i = \overline{1,n}, j = \overline{1,m}\}$ est une base de $M$ sur $K$.*

**Démonstration.**

Nous allons montrer que la famille $\{(k_i l_j) : i = \overline{1,n}, j = \overline{1,m}\}$ est une base du $K$-espace vectoriel $M$.

Cette famille est génératrice :

Soit $y$ un élément de M, Comme la famille $\{l_1, \ldots, l_m\}$ est génératrice, il existe des $\alpha_j \in L$ tels que $y = \sum_{j=1}^{m} \alpha_j l_j$ et Comme la famille $\{k_1, \ldots, k_n\}$ est génératrice, il existe pour chaque $j = \overline{1,m}$ des $\beta_{i,j} \in K$ tels que $\alpha_j = \sum_{i=1}^{n} \beta_{i,j} k_i$, On a donc

$$y = \sum_{i=1}^{n} \big( \sum_{j=1}^{m} \beta_{i,j} k_i \big) l_j = \sum_{i,j} \beta_{i,j} k_i l_j.$$

Cette famille est libre :

Supposons la relation $\sum_{i,j} \beta_{i,j} k_i l_j = 0$ avec $\beta_{i,j} \in K$ on a :

$$0 = \sum_{i,j} \beta_{i,j} k_i l_j = \sum_{j=1}^{m} \big( \sum_{i=1}^{n} \beta_{i,j} k_i \big) l_j$$

Comme la famille $(l_j)_{j=\overline{1,m}}$ est libre on a :

$$\sum_{i=1}^{n} \beta_{i,j} k_i = 0 \qquad \forall j = \overline{1,m}$$

Comme la famille $(k_i)_{i=\overline{1,n}}$ est libre on a :

$$\beta_{i,j} = 0 \qquad \forall i = \overline{1,n}, \forall j = \overline{1,m}.$$

■

**Corollaire 1.2.2**

*Si $L \subset M$ et $K \subset L$ telles que $L$ de degré fini sur $K$ et $M$ de degré fini sur $L$, alors $M$ est de degré fini sur $K$ et on a $[M : K] = [M : L].[L : K]$.*

**Démonstration.** D'apré la proposition présédent on a :
$[M : K] = Card(\{k_i l_j : i = \overline{1,n}, j = \overline{1,m}\}) = Card(\{k_1, \ldots, k_n\})Card(\{l_1, \ldots, l_m\})$

$$= [L : K][M : L].$$

■

### 1.2.2 Extension algébrique

**Définition 1.2.3**

*Soit $K \subset L$ une extension et $a \in L$, $a$ est dit algébrique sur $K$ s'il existe un polynôme non nul $P \in K[X]$ tel que $P(a) = 0$, sinon $a$ est dit transcandant.*

**Définition 1.2.4**

*Soit $K \subset L$ une extension ,si tout élément de $L$ est algébrique sur $K$, on dit que $K \subset L$ est une extension algébrique.*

**Proposition 1.2.3**

*Soient $K \subset L$ une extension de corps et $a \in L$ un élément algébrique.*
*On définit un morphisme d'anneaux $\varphi : K[X] \longrightarrow L$ ; $q \longmapsto q(a)$, on a alors :*
*(i) $\varphi$ n'est pas injectif*
*(ii) Il existe un unique polynôme unitaire $P_a$ de degré minimal vérifiant $P_a(a) = 0$ Ce polynôme est irréductible et on a $ker(\varphi) =< P_a >$ .*
*Le polynôme $P_a$ est appelé le polynôme minimal de $a$*

**Démonstration.**

$(i)$ Supposons que $a$ est algébrique sur $K$ alors il existe un polynôme non nul $P \in K[X]$ tel que $P(a) = 0$, on a $\varphi(P) = 0$ donc $P \in ker(\varphi)$ donc $ker(\varphi) \neq \{0\}$ alors $\varphi$ non injectif

$(ii)$ Soit $P_a \in ker(\varphi)$ de dégre minimal et soit $Q \in ker(\varphi)$ par la division eucludienne de $Q$ et $P_a$, $\exists S, R \in K[X]$ tels que $Q = SP_a + R$ avec $R = 0$ ou $d^\circ R < d^\circ P_a$

Si $d^\circ R < d^\circ P_a$, on a $R = Q - SP_a$ et $R(a) = 0$ donne $R \in Ker(\varphi)$ absurde et donc $R = 0$, $Q = SP_a$ et donc $ker(\varphi) =< P_a >$

Supposons que $\exists\ P_1, P_2 \in K[X]$ tels que $P_a = P_1.P_2$ donc $d^\circ P_1 < d^\circ P_a$ et $d^\circ P_2 < d^\circ P_a$ on a : $P_a(a) = P_1(a).P_2(a) = 0$ donc $P_1(a) = 0$ ou $P_2(a) = 0$ absurde avec $d^\circ P_i < d^\circ P_a;\ i = 1, 2$ donc $P_a$ irréductible.

Soit $Q \in K[X]$ unitaire de degré minimal tel que $Q(a) = 0$. si $Q - P \neq 0$ on a $(Q - P_a)(a) = 0$ avec $d^\circ(Q - P_a) < d^\circ P_a$ absurde, donc $P_a$ unique. ■

**Définition 1.2.5**

*On appelle degré de a sur K le degré de $P_a$ noté $deg_K(a)$*

**Exemple 1.2.1**

1)$a \in K \Longleftrightarrow deg_K(a) = 1$

2)$deg_{\mathbb{Q}}(\sqrt{2}) = 2$

**Définition 1.2.6**

1) *Sioent $K \subset L$ et $A$ une partie de $L$ .l'extension engendreé par $A$ est la plus petit extension de $K$ contenant $A$ et contenue dans $L$, On la note $K(A)$.*

2) *Si $A = \{a_1, a_2, \ldots, a_k\}, k \in \mathbb{N}^*$ on note $K(A) = K(a_1, a_2, \ldots, a_k)$ et on a :*

$K(A) = \left\{\frac{S(a_1,a_2,\ldots,a_k)}{T(a_1,a_2,\ldots,a_k)}; S, T \in K[X] \text{ et } T(a_1, a_2, \ldots, a_k) \neq 0\right\}$.

**Exemple 1.2.2**

*Soit $A = \{a\}$, $K(a) = \left\{\frac{S(a)}{T(a)}; S, T \in K[X] \text{ et } T(a) \neq 0\right\}$ est le plus petit sous-corps de $L$ contenant $K$ et $a$.*

**Corollaire 1.2.4**

*Soient $K \subset L$ une extension et $a \in L$, et soit $K[a] = \{q(a); q \in K[X]\}$ le plus petit sous anneau de $L$ contenant $K$ est $a$.*

*Si $a$ algébrique sur $K$ ,alors $K[a] = K(a)$ et $K[a]$ est une extension de $K$ de degré fini et $[K[a] : K] = deg_K(a)$.*

**Démonstration.**

Soit $a \in L$ algébrique de polynôme minimal $p_a$

On a $K[a] \subset K(a)$

Montrons que $K(a) \subset K[a]$

Soit $z \in K(a)$ donc $\exists\, p, q \in K[X]$ tel que $z = \frac{p(a)}{q(a)}$ avec $q(a) \neq 0$ donc $PGCD(p_a, q) = 1$ alors $\exists u, v \in K[X]$ tel que $u.p_a + v.q = 1$ on a

$$u(a).p_a(a)+v(a).q(a) = 1 \Longrightarrow q(a).v(a) = 1 \Longrightarrow p(a).q(a).v(a) = p(a) \Longrightarrow p(a).v(a) = \frac{p(a)}{q(a)} = z$$

donc $z \in K[a]$ alors $K[a] = K(a)$

Soit $z = T(a) \in K[a]$, il existe $q, r \in K[X]$ tels que $T = p_a q + r$ et tel que $d^\circ r < d^\circ p_a \vee r = 0$ et donc $z = T(a) = r(a)$

Si on pose $r = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}; a_i \in K, n = d^\circ p_a$

On aurit $z = a_0 + a_1 a + \ldots + a_{n-1} a^{n-1}$ donc $\{1, a, \ldots, a^{n-1}\}$ est une partie generatrice du $K$-espace vectoriel $K[a]$.

Montrons que $\{1, a, \ldots, a^{n-1}\}$ est libre.

Soient $\lambda_0, \ldots, \lambda_{n-1} \in K$ tels que $\lambda_0 + \lambda_1 a^{n-1} + \ldots + \lambda_{n-1} a^{n-1} = 0$.

S'il existe $i_0 = \overline{0, n-1}$ tel que $\lambda_{i_0} \neq 0$, le polynôme $S = \lambda_0 + \lambda_1 X^{n-1} + \ldots + \lambda_{n-1} X^{n-1}$ est non nul appartient à $K[X]$ et verifie $S(a) = 0$ avec $d^\circ S < d^\circ p_a$ absurde. D'ou $\lambda_i = 0\ \forall i = \overline{0, n-1}$ et donc $\{1, a, \ldots, a^{n-1}\}$ est libre. ■

**Proposition 1.2.5**

*Toute extension de degré fini est algébrique.*

**Démonstration.**

Soit $K \subset L$ de degré fini et soit $a \in L$, La famille $\{1, a, \ldots, a^n\}$ est liée dans $L$, donc il existe des éléments non tous nuls $\alpha_0, \ldots, \alpha_n \in K$ tel que $\alpha_0 + \ldots + \alpha_n a^n = 0$

Le polynôme $P(X) = \alpha_0 + \ldots + \alpha_n X^n \in K[X]; P \neq 0$ et $P$ s'annule en $a$. donc $a$ est algébrique sur $K$. ■

**Corollaire 1.2.6**

*Le ensemble $\overline{K}$ des éléments de $L$ algébriques sur $K$ est une extension de $K$.*

**Démonstration.**

Soient $a, b \in \overline{K}$ on a, $a.b, a + b$ et $a^{-1}$ dans $K(a, b)$ qui est de degré fini, donc algébrique .

Alors $a.b, a+b, a^{-1}$ sont algébriques sur $K$ donc $K \subset \overline{K}$ est uneextension de $K$. ■

**Corollaire 1.2.7**

*Soient $A, B$ deux parties de $L$. Alors on a :*
$K(A \cup B) = K(A)(B)$

**Théorème 1.2.8**

*Soit $K \subset L$ une extension de corps. Alors $L$ est de degré fini si et seulement s'il existe $x_1, \ldots, x_n \in L$, algébriques sur $K$, tels que $L = K(x_1, \ldots, x_n)$.*

**Démonstration.**

Si $L$ est de degré fini, alors elle est algébrique.
Soient $x_1, \ldots, x_n \in L$, une base de $L$ sur $K$, les $x_i$ sont tous algébriques sur $K$ et
$L = K(x_1, \ldots, x_n)$.
Réciproquement, si $L = K(x_1, \ldots, x_n)$, avec tous les $x_i$ algébriques sur $K$, montrons que $L$ est de degré fini.
Procédons par récurrence sur $n$ :
Le cas $n = 1$ a partir de corollaire 1.2.4 $L$ est de degré fini.
Supposons la propriété vraie pour une valeur de $n$.
d'aprés le corolaire 1.2.7, $K(x_1, \ldots, x_{n+1}) = K(x_1, \ldots, x_n)(x_{n+1})$
Ainsi, $x_{n+1}$, étant algébrique sur $K$, est algébrique sur $K(x_1, \ldots, x_n)$, donc d'après corollaire 1.2.4 $K(x_1, \ldots, x_n) \subset K(x_1, \ldots, x_n, x_{n+1})$ est de degré fini ainsi que $K \subset K(x_1, \ldots, x_n)$ par hypothèse de récurrence, et la formule de multiplicativité des degrés donne $K \subset K(x_1, \ldots, x_n, x_{n+1})$ est de degré fini. ■

**Proposition 1.2.9**

*Soit $K \subset L$ une extension algébrique de $K$ et $K \subset M$ une extension de $K$.*
*(i) Un élément $x \in M$ est algébrique sur $K$ si et seulement si $x$ est algébrique sur $L$.*
*(ii) $M$ est une extension algébrique sur $K$ si et seulement si $M$ est une extension algébrique de $L$.*

### 1.2.3 Corps de rupture

**Définition 1.2.7**

*Soit $P$ un polynôme irréductible de $K[X]$.*
*On dit qu'une extension $L$ de $K$ est un corps de rupture pour $P$ sur $K$ s'il existe une racine $a$ de $P$ dans $L$ telle que $L = K[a]$.*

**Théorème 1.2.10**

*Pour tout polynôme irréductible $P \in K[X]$, il existe un corps de rupture $L$. De plus si $L^{'}$ est un autre corps de rupture pour $P$ alors $L$ et $L^{'}$ sont $K$-isomorphismes.*

**Démonstration.**

Comme $P$ est irréductible, $L = K[X]/ < P >$ est un corps. C'est une extension de K car l'application $\varphi : K \longrightarrow L;\ \lambda \longmapsto \overline{\lambda}$ est un morphisme de corps.

Si on prend pour $a$ la classe de $X$ dans $K[X]/ < P >$, on a $P(a) = 0$ et $L = K[a]$, donc $L$ est un corps de rupture pour $P$ sur $K$. D'où l'existence.

Si $L^{'}$ est un corps de rupture pour $P$ sur $K$, soit $a^{'}$ avec $L^{'} = K[a^{'}]$ et $P(a^{'}) = 0$.

Alors l'application $\phi : K[X] \longrightarrow L^{'};\ Q \longmapsto Q(a^{'})$ est surjective, $ker\phi =< P >$ car $ker\phi$ contient $P$ avec $P$ irréductible .

On a $K[X]/ker\phi \simeq K[a^{'}]$ donc $L = K[X]/ < P >\simeq L^{'}$. ■

### 1.2.4 Corps de décomposition

**Définition 1.2.8**

*Soient $K$ un corps et $P \in K[X]$. On dit qu'une extension $K \subset L$ est un corps de décomposition pour $P$ sur $K$ si $L$ est engendré par les racines de $P$ sur $L$.*

**Exemple 1.2.3**

- *Le corps $\mathbb{C}$ est un corps de décomposition sur $\mathbb{R}$ pour le polynôme $X^2 + 1$.*
- *Le corps $\mathbb{Q}[\sqrt{2}]$ est un corps de décomposition sur $\mathbb{Q}$ pour le polynôme $X^2 - 1$.*

**Théorème 1.2.11**

*Tout polynôme non nul $P$ de $K[X]$ possède un corps de décomposition.*

**Démonstration.**

Montrer par récurrence sur le degré $n$ de $P$

Si $n = 1$ alors $K$ est un corps de décomposition pour $P$ sur $K$

Supposons le théorème vrai pour tout polynôme de degré $< n$ et démontrons pour les polynômes de degré $n$

on a il existe une extension $L$ de $K$ contenant une racine $a$ de $P$ donc $P = (X - a)Q(X)$ avec $degQ = n - 1$, L'hypothèse de récurrence nous permet de trouver un corps de décomposition $K_1$ pour $Q(X)$ alors

$$Q(X) = \prod_{i=1}^{n-1}(X - a_i)$$

dans $K_1[X]$, et donc

$$P(X) = (X - a)\prod_{i=1}^{n-1}(X - a_i) = \prod_{i=0}^{n-1}(X - a_i)$$

dans $K_1[a][X]$ ou $a_0 = a$.
donc $K_1[a][X]$ est un corps de décomposition pour $P$ sur $K$. ■

**Corollaire 1.2.12**

*Soit $L, L'$ deux corps de décomposision de $P$ sur $K$. Alors il existe un isomorphisme de $L$ sur $L'$.*

### 1.2.5 Clôture algébrique

**Définition 1.2.9**

*Un corps commutatif $K$ est dit algébriquement clos si tout polynôme à coefficients dans $K$, admet (au moins) une racine dans $K$.*
*c'est un corps qui n'a pas d'extension algébrique propre.*

**Définition 1.2.10**

*Une clôture algébrique d'un corps commutatif $K$ est une extension algébrique $L$ de $K$ algébriquement close.*

**Théorème 1.2.13 (Lie kolchin)** *[3]*

*Soient $C$ un corps algébriquement clos et $G \subset GL(n, C)$ un groupe résoluble, alors il existe une base $\{\underline{v_1}, \ldots, \underline{v_n}\}$ de $C$-espace vectoriel $C^n$ lelle que :*

$$A\underline{v_i} = \lambda_{i,1}\underline{v_1} + \ldots + \lambda_{i,n}\underline{v_n}$$

*pour tout $\lambda_{i,j} \in C; 1 \leq i, j \leq n$, et $A \in G$.*

### 1.2.6 Théorème de l'élément primitif

**Lemme 1.2.14**

*Soit $K \subset L$ une extension, avec $K$ de caractéristequr nulle et $x \in L$ algébrique sur $K$ de polynôme minimal $P_x \in K[X]$. Alors $x$ est racine simple de $P_x$.*

**Démonstration.**

Soit $x \in L$ un racine multiple de $P_x$. Alors le polynôme derivé $P'_x \neq 0$ verifie
$P'_x(x) = 0$ et $d^\circ P'_x < d^\circ P_x$, absurde. ■

**Théorème 1.2.15**

*Soit $K \subset L$ une extension de degré fini où $K$ est de caractéristique nulle. Alors, il existe $a \in L$ tel que $L = K(a)$.*

**Démonstration.**

Comme $L$ de degré fini alors elle est engendrée par un nombre fini d'éléments algébriques
On suppose que $L = K[x, y]$, on cherche $a = x + ty$ avec $t \in K$
soient $P$ le polynôm minimal de $x$ et $Q$ le polynôm minimal de $y$, $P$ et $Q$ se décomposent sur leur corps de décomposition :

$$P = \prod_{i=1}^{n}(X - \alpha_i), \qquad Q(X) = \prod_{j=1}^{m}(X - \beta_j)$$

avec $\alpha_1 = x$ et $\beta_1 = y$
Puisque $P$ et $Q$ sont irréductibles sur $K$ de caractéristique nulle, leurs racines sont simples donc les $\alpha_i$ et les $\beta_j$ sont deux à deux distincts
comme $K$ est infini,on peut trouver $t \in K$ tel que $t \neq \frac{x-\alpha_i}{y-\beta_j}$ pour tout $i$ et $j \neq 1$
posant $a = x + ty$, on a :

$$P(a - ty) = P(x) = 0,$$

les polynômes $Q(X)$ et $P(a-tX)$ dans $K[X]$ ont donc une unique racine commune à savoir $y$ et leur pgcd est ainsi $X-y$ irréductible est le polynôme minimal de $y$ sur $K(a)$ donc $y \in K(a)$, mais $x = a-ty \in K(a)$ donc $L = K(a)$. ∎

### 1.2.7 Extensions normales et galoisiennes

**Définition 1.2.11**

*Soient $K \subset L_1, K \subset L_2$ deux extensions de $K$ contenues dans $\mathbb{C}$ . On appelle $K$-homomorphisme de $L_1$ dans $L_2$ un homomorphisme d'anneaux $\delta : L_1 \longrightarrow L_2$ qui est l'identité sur $K$.*
*Un $K$-automorphisme de $L$ est un automorphisme de corps $L \longrightarrow L$ qui est l'identité sur $K$.*

**Définition 1.2.12**

*Soit $K$ un corps et $P \in K[X]$ un polynôme irréductible.*
*(i) On dit que $P$ est séparable si $P$ ne posséde que des racines simples dans $K$.*
*(ii) Un élément algébrique $a$ d'une extension $K \subset L$ est dit séparable, si $P_a$ est un polynôme séparable.*
*(iii) Une extension algébrique $K \subset L$ est dite séparable si tous les éléments de $L$ sont séparables.*

**Définition 1.2.13**

*Soit $P \in K[X]$ et $a$ une racine de $P$, on appelle conjugué de $a$ toute racine de $P$.*

**Définition 1.2.14**

*On dit qu'une extension algébrique $K \subset N$ est normale si les conjugués de tous les éléments de $N$ sont dans $N$.*

**Proposition 1.2.16**

*Si $K$ est de caractéristique zéro et si $K \subset N$ est une extension on a alors :*
*$K \subset N$ normal $\Longleftrightarrow$ tout $K$-homomorphisme est un $K$- automorphisme.*

**Proposition 1.2.17**

*Soient $K \subset L$ et $L \subset M$ deux extensions algébriques. Si $K \subset M$ est normale, alors $L \subset M$ est normale.*

**Démonstration.** Si $b$ est un conjugué sur $K$ d'un élément $a \in M$, alors c'est aussi un conjugué sur $L$, car le polynôme minimal de $a$ dans $L$ divise le polynôme minimal de $a$ dans $K$. ■

**Définition 1.2.15**

*Une extension algébrique $K \subset L$ est dite galoisienne, si elle est normale et séparable.*

## 1.3 Groupe de Galois d'une extension

**Définition 1.3.1**

*Soit $K \subset L$ une extension de corps. Le groupe de Galois $Gal(L/K)$ est le groupe des $K$-automorphismes de $L$.*

**Proposition 1.3.1**

*Si $K \subset L$ une extension algébrique de degré fini. Alors :*
*(i) $|Gal(L/K))| \leq [L : K]$.*
*(ii) $|Gal(L/K)| = [L : K]$ si et seulement si l'extension $K \subset L$ est normale.*

**Proposition 1.3.2**

*Soit $K \subset L$ une extension de corps et soit $H$ un sous-groupe de $Gal(L/K)$ l'ensemble $M = L^H = \{x \in L;\ \varphi(x) = x\ \forall \varphi \in H\}$ est une extension de $K$ contenue dans $L$.*

**Démonstration.**

Monrons que $L^H = M$ est un sous corps de $L$

(1) $(M, +)$ un groupe, on a :

*i*) $\forall \varphi \in H,\ \varphi(0_L) = 0_L$ donc $0_L \in M$

*ii*) soient $x, y \in M$ donc $\forall \varphi \in H, \varphi(x) = x; \varphi(y) = y$ on a :

$\varphi(x + y) = \varphi(x) + \varphi(y) = x + y$ donc $x + y \in M$.

*iii*) soit $x \in M$ donc $\forall \varphi \in H; \varphi(x) = x$ on a :

$0 = \varphi(x + (-x)) = \varphi(x) + \varphi(-x)$ donc $\varphi(-x) = -\varphi(x) = -x$ donc $-x \in M$

(2) soient $x, y \in M$ donc $\forall \varphi \in H, \varphi(x) = x; \varphi(y) = y$ on a :

$\varphi(xy) = \varphi(x)\varphi(y) = xy$ donc $xy \in M$.

(3) ona $\forall \varphi \in H, \varphi(1_L) = 1_L$ donc $1_L \in M$

(4) soit $x \in M - \{0\}$ donc $\forall \varphi \in H \varphi(x) = x$ on a :

$1 = \varphi(x.x^{-1}) = \varphi(x)\varphi(x^{-1})$ donc $\varphi(x^{-1}) = (\varphi(x))^{-1} = x^{-1}$ donc $x^{-1} \in M$.

donc $M$ est un sous corps de $L$ donc $K \subset M$ est une extension . ■

# Chapitre 2

# Algèbre Différentiel

Ce chapitre est une introduction à la théorie de Galois différentiel ou on trouve des éléments concernant les corps différentiels, qui nous seront utiles pour introduire une extension de Picard-Vessiot associée à un système différentiel linéaire d'ordre un, qui à son tour nous permet de définir le groupe de Galois différentiel.

## 2.1 Rappels sur l'algèbre différentiel

### 2.1.1 Anneaux et Corps différentiel

**Définition 2.1.1**

*Un anneau différentiel $(A, \delta)$ est un anneau commutatif $A$ muni d'une dérivation $\delta : A \longrightarrow A$ vérifiant :*

$(i)\ \delta(a+b) = \delta(a) + \delta(b),\ \forall a, b \in A$

$(ii)\ \delta(ab) = \delta(a)b + \delta(b)a,\ \forall a, b \in A$

*Dans le cas où $A$ est un corps , $(A, \delta)$ est appelé corps différentiel.*

**Définition 2.1.2**

*Un idéal $I$ d'un anneau différentiel $A$ est dit idéal différentiel s'il est stable par la dérevation $\delta$, c'est à dire si $\delta(I) \subseteq I$.*

**Définition 2.1.3**

*Soient $(A_1, \delta_1)$ et $(A_2, \delta_2)$ deux anneaux différentiels*

*Un morphisme d'anneaux différentiels est $f : (A_1, \delta_1) \longrightarrow (A_2, \delta_2)$ est un morphisme d'anneaux $f : A_1 \longrightarrow A_2$ qui satisfait $f(\delta_1(a)) = \delta_2(f(a)),\ \forall a \in A_1$.*

*Si le morphisme $f$ est injectif, on dira que $(A_2, \delta_2)$ est une extension différentielle de $(A_1, \delta_1)$ via $f$.*

**Exemple 2.1.1**

*Le noyau d'un morphisme d'anneaux différentiels est un idéal différentiel.*

**Proposition 2.1.1**

*Soit $I$ un idéal différentiel de $A$.*

*L'anneau $A/I$ est un anneau différentiel tel que la surjection canonique $\pi : A \longrightarrow A/I$ soit un morphisme d'anneaux différentiels.*

**Démonstration.**

On sait que $A/I$ est muni la structure d'anneau pour les lois $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a}\overline{b} = \overline{ab}$
$\forall\ \overline{a}, \overline{b} \in A/I$. Soit :

$$\begin{aligned} \delta_0 : A/I &\longrightarrow A/I \\ \overline{a} &\longmapsto \delta_0(\overline{a}) = \overline{\delta(a)}. \end{aligned}$$

$\delta_0$ est bien une application, En effet :
Soient $\overline{a}, \overline{b} \in A/I$ tels que $\overline{a} = \overline{b}$

$$\begin{aligned} \overline{a} = \overline{b} &\Longrightarrow a - b \in I \\ &\Longrightarrow \delta(a-b) \subset \delta(I) \subset I \\ &\Longrightarrow \delta(a) - \delta(b) \in I \\ &\Longrightarrow \overline{\delta(a)} = \overline{\delta(b)} \\ &\Longrightarrow \delta_0(\overline{a}) = \delta_0(\overline{b}) \end{aligned}$$

On a :

• $\delta_0(\overline{a} + \overline{b}) = \delta_0(\overline{a+b}) = \overline{\delta(a+b)} = \overline{\delta(a) + \delta(b)} = \overline{\delta(a)} + \overline{\delta(b)} = \delta_0(\overline{a}) + \delta_0(\overline{b})$.

• $\delta_0(\overline{a}.\overline{b}) = \delta_0(\overline{a.b}) = \overline{\delta(a.b)} = \overline{b.\delta(a) + a.\delta(b)} = \overline{b}.\overline{\delta(a)} + \overline{a}.\overline{\delta(b)} = b.\delta_0(\overline{a}) + a.\delta_0(\overline{b})$.

d'où $\delta_0$ est une dérivation.

Soient $\overline{a}, \overline{b} \in A/I$, et $\pi : A \longrightarrow A/I$ tel que $\pi(a) = \overline{a}$ le morphisme canonique d'anneaux. On a
$\delta_0(\pi(a)) = \delta_0(\overline{a}) = \overline{\delta(a)} = \pi(\delta(a))$

d'ou $\pi$ est un morphisme d'anneaux différentiels. ∎

**Définition 2.1.4**

*Un anneau différentiel $A$ est simple si les seuls idéaux différentiels de $A$ sont $\{0\}$ et $A$.*

**Définition 2.1.5**

*Un élément $a \in A$ est dit constante si $\delta(a) = 0$.*

*On note par $Const(A)$ l'ensemble des constantes de $A$.*

**Proposition 2.1.2**

*L'ensemble $Const(A) = \{a \in A : \delta(a) = 0\}$ est un sous anneau (sous corps si $A$ est un corps) de $A$ appelé sous anneau des constantes.*

**Démonstration.**

Soit $A$ un anneau

1)$(Const(A), +)$ sous groupe :

• On a $0 \in Const(A)$ car $\delta(0) = \delta(0 + 0) = \delta(0) + \delta(0) \Longrightarrow \delta(0) = 0$.

• Soient $a, b \in Const(A)$ on a $\delta(a + b) = \delta(a) + \delta(b) = 0 + 0 = 0$

donc $a + b \in Const(A)$.

• Soit $a \in Const(A)$ on a $\delta(a + (-a)) = \delta(a) + \delta(-a)$ et $\delta(a + (-a)) = \delta(0) = 0$

donc $\delta(a) + \delta(-a) = 0$ alors $\delta(-a) = -\delta(a) = 0$ donc $-a \in Const(A)$.

Donc $Const(A)$ est un sous group de $(A, +)$.

2) $1 \in Const(A)$ car $\delta(1) = \delta(1.1) = 1.\delta(1) + \delta(1).1 = \delta(1) + \delta(1) \Longrightarrow \delta(1) = 0$.

3) Soit $a, b \in const(A)$ on a $\delta(a.b) = b.\delta(a) + a.\delta(b) = b.0 + a.0 = 0$ donc $a.b \in const(A)$.

Donc $const(A)$ est un sous anneau de $A$. ■

## 2.1.2 Proprietés des anneaux et corps différentiels

**Proposition 2.1.3**

*Soit $(A, \delta)$ un anneau différentiel intégre et soit $K$ son corps de fractions. Il existe une unique dérivation sur $K$ qui coinside avec $\delta$ sur $A$ et donc $K$ a une structure de corps différentiel.*

**Démonstration.**

Soit $x \in K$, il existe $a, b \in A$ tel que $x = \frac{a}{b}$ $/b \neq 0$, on pose $\delta_1(x) = \frac{\delta(a).b - a.\delta(b)}{b^2}$

on verifie que $\delta_1$ est une application :

Soient $\frac{a}{b}, \frac{c}{d} \in K$ tel que $\frac{a}{b} = \frac{c}{d}$, ce ci est equivalent à $ad = bc$,

il suffit de montre que $\delta_1(\frac{at}{bt}) = \delta_1(\frac{a}{b})$ $\forall t \in A - \{0\}$.

Soit $t \in A - \{0\}$

$$\begin{aligned}\delta_1\Big(\frac{at}{bt}\Big) &= \frac{\delta(at).bt - at.\delta(bt)}{(bt)^2}\\ &= \frac{abt\delta(t) + bt^2\delta(a) - at^2\delta(b) - abt\delta(t)}{b^2t^2}\\ &= \frac{t^2(\delta(a).b - a.\delta(b))}{b^2t^2} = \delta_1\Big(\frac{a}{b}\Big)\end{aligned}$$

donc $\forall t \in A - \{0\},\ \delta_1(\frac{at}{bt}) = \delta_1(\frac{a}{b})$

donc $\delta_1(\frac{ad}{bd}) = \delta_1(\frac{a}{b})$ et $\delta_1(\frac{ad}{bd}) = \delta_1(\frac{bc}{bd}) = \delta_1(\frac{c}{d}),$ d'ou $\delta_1(\frac{a}{b}) = \delta_1(\frac{c}{d})$

donc $\delta_1$ est une application.

Soient $\frac{a}{b}, \frac{c}{d} \in K,$ on a :

$$\begin{aligned}\delta_1\Big(\frac{a}{b} + \frac{c}{d}\Big) &= \delta_1\Big(\frac{ad + bc}{bd}\Big)\\ &= \frac{\delta(ad + bc)bd - \delta(bd)(ad + bc)}{b^2d^2}\\ &= \frac{\delta(ad)bd + \delta(bc)bd - \delta(bd)ad - \delta(bd)bc}{b^2d^2}\\ &= \frac{\delta(ad)bd - \delta(bd)ad}{b^2d^2} + \frac{\delta(bc)bd - \delta(bd)bc}{b^2d^2}\\ &= \delta_1\Big(\frac{ad}{bd}\Big) + \delta_1\Big(\frac{bc}{bd}\Big) = \delta_1\Big(\frac{a}{b}\Big) + \delta_1\Big(\frac{c}{d}\Big).\end{aligned}$$

et

$$\begin{aligned}\delta_1(\frac{a}{b}.\frac{c}{d}) &= \frac{\delta(ac)bd - \delta(bd)ac}{b^2d^2}\\ &= \frac{\delta(a)cbd + \delta(c)abd - \delta(b)dac - \delta(d)bac}{b^2d^2}\\ &= \frac{\delta(a)cbd - \delta(b)adc}{b^2d^2} + \frac{\delta(c)dab - \delta(d)bac}{b^2d^2}\\ &= cd\left(\frac{\delta(a)b - \delta(b)a}{b^2d^2}\right) + ab\left(\frac{\delta(c)d - \delta(d)c}{b^2d^2}\right)\\ &= \frac{c}{d}\Big(\delta_1\Big(\frac{a}{b}\Big)\Big) + \frac{a}{b}\Big(\delta_1\Big(\frac{c}{d}\Big)\Big).\end{aligned}$$

Donc $\delta_1$ est une dérivation. ■

**Théorème 2.1.4**

*Soit $(A, \delta)$ un anneau différentiel et soit $A[x]$ l'anneau des polynômes en une indeterminée sur $A$.*

*Pour tout $P \in A[x]$, il existe une unique dérivation $\delta_p$ de $A[x]$ qui étend $\delta$ telle que $\delta_p(x) = P$ et telle que le morphisme canonique $A \longrightarrow A[X]$ soit un morphisme d'anneaux différentiels .*

**Démonstration.**

Soit $q = \sum_{k=0}^{n} a_k X^k$ un élément de $A[X]$ :

$$\begin{aligned}\partial(q) &= \sum_{k=0}^{n} \partial(a_k X^k) \\ &= \sum_{k=0}^{n} \partial(a_k) X^k + \partial(X^k) a_k \\ &= \sum_{k=0}^{n} \partial(a_k) X^k + (\sum_{k=0}^{n} k a_k X^{k-1}) \partial(X) \\ &= q^{\delta}(X) + q'(X)\partial(X)\end{aligned}$$

ou $q^{\delta}(X) = \sum_{k=0}^{n} \partial(a_k) X^k$

Donc une dérivation $\partial$ sur $A[X]$ qui etend $\delta$ est determinée par l'image $\partial(X)$.

Réciproqument, Pour $P \in A[X]$, l'application définie par :$\partial(X) = P$ et

$$\partial(q) = q^{\delta}(X) + Pq'(X) = \sum_{k=0}^{n} \partial(a_k) X^k + P \sum_{k=0}^{n} k a_k X^{k-1}$$

définit une dérivation sur $A[X]$ qui étend $\delta$, notée $\delta_p$. ∎

**Théorème 2.1.5**

*Soit $(K, \delta)$ un corps diffirentiel de caractéristique nulle et soit $L$ une extension algébrique de degré fini, il existe alors une uniqe dérivation sur $L$ qui étend $\delta$.*

**Démonstration.**

Commme $K$ est de caractéristique nulle et $K \subset L$ une extension algébrique de degré fini donc d'aprés le théoréme 1.2.15 il existe un élément $x$ de $L$ tel que $L = K[x]$. Soit $P_0 = \sum_{k=0}^{n} a_k X^k$ le polynôme minimal de $x$

d'aprés le théoréme 1.2.10 $L \simeq K[X]/ < P_0 >$, si $\delta_L$ est une dérivation qui étent $\delta$, en dérivant la relation $P_0 = 0$,on obtient :

$$\begin{aligned}0 = \delta_L(P_0(x)) &= \sum_{k=0}^{n} \delta(a_k) x^k + \sum_{k=0}^{n} k a_k x^{k-1} \delta_L(x) \\ &= P_0^{\delta}(x) + P_0^{'}(x)\delta_L(x)\end{aligned}$$

donc $\delta_L(x) = -\frac{P_0^{\delta}(x)}{P_0^{'}(x)}$ $\qquad (*)$

Montrons que cette dérivation existe. on a d'aprés le théoréme 1.2.10 $L \simeq K[X]/ < P_0 >$ où $< P_0 >= ker(\varphi)$ donc il suffit de montrer qu'il existe une dérevation sur $K[X]$ tell que $< P_0 >$ soit idéal différentiel ce qui induit une dérivation sur $K[X]/ < P_0 >$ et donc sur $L$.
Si $\partial$ est une dérivation sur $K[X]$, on avu que $\forall\ Q \in K[X]; \partial(Q) = Q^{\delta} + Q^{'}\partial(Q)$ donc $\partial(P_0(X)) = P_0^{\delta} + P_0^{'}\partial(X)$, comme $P_0$ est séparaple donc $P_0$ et $P_0^{'}$ premiers entre eux et donc il existe deux polynômes $S, T$ dans $K[X]$ tel que $SP_0 + TP_0^{'} = 1$ donc $TP_0^{'}(x) = 1$ alors $P_0^{'}(x) = \frac{1}{T(x)}$
en considéreant $(*)$ il suffit de poser $\partial(X) = -\frac{P_0^{\delta}}{P_0^{'}} = -TP_0^{\delta}$, qui définit une dérivation sur $K[X]$ et telle que

$$\begin{aligned}\partial(P_0(X)) = P_0^{\delta} + P_0^{'}\partial(X) = P_0^{\delta} + P_0^{'}(-TP_0^{\delta}) &= P_0^{\delta} - P_0^{'}TP_0^{\delta} \\ &= P_0^{\delta}(1 - P_0^{'}T) \\ &= P_0^{\delta}SP_0 \\ &= (SP_0^{\delta})P_0\end{aligned}$$

donc $\partial(P_0(X)) \in < P_0 >$ et donc $< P_0 >$ est un idéal différentiel de $K[X]$
donc $\partial_L$ induit une dérivation sur $K[X]/ < P_0 >$ et donc sur $L$. ■

**Théorème 2.1.6**

*Soient $(K, \delta)$ un corps différentiel et $K \subset L$, $K \subset M$ deux extensions différentielles, alors $L \otimes_K M$ est muni de la dérivation*

$$\delta(\sum b_i \otimes c_i) = \sum(\delta(b_i) \otimes c_i + b_i \otimes \delta(c_i));\ b_i \in L, c_i \in M.$$

### 2.1.3 Equations différentielles linéaires

Pour tout $a \in (K, \delta)$ on note $a' = \delta(a), a'' = \delta(\delta(a)), ..., a^{(n)} = \delta^n(a)$ avec $a = a^0 = \delta^0(a)$.

**Définition 2.1.6**

*Soit $(K, \delta)$ un corps différentiel*

*Un système différentiel d'ordre un et de rang n sur le corps différentiel K est donné par :*

$$\begin{pmatrix} y_1' \\ y_2' \\ \vdots \\ y_n' \end{pmatrix} = A \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

*Où $A = (a_{i,j}) \in M_n(K)$ et $y_1, y_2, \cdots, y_n$ sont des indéterminées différentielles sur $K$.*
*On notera ce système par $(\Delta_A)$.*

**Définition 2.1.7**

*Soit $K \subseteq F$ une extension différentielle d'anneaux*
*l'ensemble des solutions du système différentiel $(\Delta_A)$. à valeurs dans $F$ est l'ensemble*

$$Sol_F(\Delta_A) = \{f^t = (f_1, \ldots, f_n)^t \in F^n : f_i' = \sum_{j=1}^{n} a_{i,j} f_j,\ i = \overline{1,n}\ \}.$$

**Remarque 2.1.1**

*La somme de deux solutions est une solution, et le produit d'une solution par une constante est une solution, donc $Sol_F(\Delta_A)$ est un module sur l'anneau $Const(F)$.*
*Si $F$ est un corps, alors $Sol_F(\Delta_A)$ est un espace vectoriel sur $Const(F)$.*

**Proposition 2.1.7**

*Si $M = (m_{i,j})$ est une matrice à coeffcients dans un anneau différentiel $K$, on note $M' = (m'_{i,j})$.*
*On a :*

$$(MN)' = M'N + MN'.$$

**Démonstration.**

Soient $M = (a_{i,j})$ et $N = (b_{i,j})$ de $M_n(K)$ on a :

$$\begin{aligned}(MN)' = \Big(\sum_{k=1}^{n} a_{i,k} b_{k,j}\Big)' &= \sum_{k=1}^{n} (a_{i,k} b_{k,j})' \\ &= \sum_{k=1}^{n} a'_{i,k} b_{k,j} + a_{i,k} b'_{k,j} \\ &= \sum_{k=1}^{n} a'_{i,k} b_{k,j} + \sum_{k=1}^{n} a_{i,k} b'_{k,j} \\ &= M'N + MN'.\end{aligned}$$

■

• On note $GL(n, K)$ le groupe des matrices carées â coeffcients dans $K$, inversibles dans $K$

**Proposition 2.1.8**

$\forall M \in GL(n, K)$ *On a :*

$$(M^{-1})' = -M^{-1} M' M^{-1}.$$

**Démonstration.** Soit $M \in GL(n, K)$
En dérivant l'égalité $MM^{-1} = I_n$ on a :

$$0 = (I_n)' = (MM^{-1})' = M'M^{-1} + M(M^{-1})'$$

donc $M(M^{-1})' = -M'M^{-1}$, alors $(M^{-1})' = -M^{-1}M'M^{-1}$. ∎

**Définition 2.1.8**
*Une matrice fondamentale pour le système $(\Delta_A)$ â coeffcients dans $F$ est une matrice $U \in GL(n, F)$ telle que $U' = AU$.*

**Proposition 2.1.9**
*Soient $U, V \in GL(n, F)$ deux matrices fondamentales pour le systéme $(\Delta_A)$.*
*Alors, il existe une unique matrice $C \in GL(n, Const(F))$, telle que : $U = V.C$.*

**Démonstration.**
En dérivant $V^{-1}U$ on obtient

$$\begin{aligned}(V^{-1}U)' &= (V^{-1})'U + V^{-1}U' \\ &= -V^{-1}V'V^{-1}U + V^{-1}U \\ &= -V^{-1}AVV^{-1}U + V^{-1}AU = 0\end{aligned}$$

Alors $C = V^{-1}U \in GL(n, Const(F))$. ∎

**Corollaire 2.1.10**
*Soit $(\Delta_A)$ un systéme différentiel $Y' = A.Y$.*
*Soit $Q \in GL(n, K)$ telle que : $Z = Q.Y$ .$Y$ est un solution de $(\Delta_A)$ si et seulement si $Z$ est solution de $\Delta_{Q_A}$, où $Q_A = Q'.Q^{-1} + Q.A.Q^{-1}$.*

**Démonstration.** On a $Z = QY$ donc :

$$\begin{aligned}Z' = (QY)' &= Q'.Y + Q.Y' \\ &= Q'.Y + Q.A.Y \\ &= Q'.Q^{-1}Q.Y + Q.A.Q^{-1}Q.Y \\ &= Q'.Q^{-1}.Z + Q.A.Q^{-1}.Z \\ &= (Q'.Q^{-1} + Q.A.Q^{-1})Z = Q_AZ.\end{aligned}$$

Résiproquement

$$\begin{aligned} Z' = Q_A Z \Longrightarrow (QY)' = Q_A QY &\Longrightarrow Q'.Y + QY' = (Q'.Q^{-1} + Q.AQ^{-1})QY \\ &\Longrightarrow Q'Y + QY' = Q'Y + QAY \\ &\Longrightarrow QY' = QAY \\ &\Longrightarrow Y' = AY. \end{aligned}$$

Si $U \in GL(n, Const(K))$ un matrice fondamentale de $\Delta_A$ on a :

$$\begin{aligned} (QU)' &= Q.U' + Q'.U = Q.A.U + Q'.U \\ &= Q'.Q^{-1}.Q.U + Q.A.Q^{-1}.Q.U \\ &= (Q'Q^{-1} + Q.A.Q^{-1}).QU \\ &= Q_A.QU. \end{aligned}$$

donc $QU$ est une matrice fondamentale de $(\Delta_{Q_A})$. ■

**Définition 2.1.9**

*Le wronskien de n éléments $(y_1, \ldots, y_n)$ dans un anneau différentiel est le déterminant*

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

**Lemme 2.1.11**

*Les éléments $\{y_1, \ldots, y_n\}$ sont linéairment indépendant si et seulment si leur wronskien est non nul.*

**Proposition 2.1.12**

*Soit $F$ un corps.*

*Le $Const(F)$-espace vectoriel $Sol_F(\Delta_A)$ est de dimension Inférieur ou égal à $n$.*

**Démonstration.**

Supposons qu'on a $n+1$ solutions $f_1^t, \ldots, f_{n+1}^t \in F^n$ linéairement indépendants sur $Const(F)$.

On considére les matrices $U = [f_1^t, \ldots, f_n^t]$, $V = [f_2^t, \ldots, f_{n+1}^t]$

Comme les colonnes de $U$ et $V$ sont des solutions donc $U$ et $V$ sont matrices fondamentales

pour $(\Delta_A)$, en effet :
Supposons $det(U) = 0$. Alors il existe $\lambda = (\lambda_1, \ldots, \lambda_n) \neq 0 \in F^n$, tel que $U\lambda^t = 0$.
On choisit $\lambda$ de tel sorte qu'il soit minimal en le nombre des composantes différentes de zéro.
Il existe une composante $\lambda_k \neq 0$. On divise par $\lambda_k$, et on peut supposer que $\lambda_k = 1$ En dérivant l'égalité $U.\lambda^t = 0$ on obtient :

$$0 = U^{'}.\lambda^t + U.(\lambda^t)^{'} = A.U.\lambda^t + U.(\lambda^t)^{'} = U.(\lambda^t)^{'}$$

Le nombre des composantes différentes de zéro de $\lambda^{'}$ est plus petit que celui de$\lambda$. Par la minimalité de $\lambda$ on a $\lambda^{'} = 0$. Alors $f_1^t, \ldots, f_n^t$ sont linéairement dépendantes sur $Const(F)$, ce qui contredit notre hypothése d'ou $det(U) \neq 0$.
De la méme façon on montre $det(V) \neq 0$.
Par le lemme précédent il existe une matrice des constantes $C$ telle que $U = V.C$. Alors $f_{n+1}^t$ dépend linéairement $f_1^t, \ldots, f_n^t$ sur $Const(F)$. donc les solutions $f_1^t, \ldots, f_{n+1}^t$ sont linéarment indépendantessont sur $Const(F)$ alors $\dim_{Const(F)}(sol_F(\Delta_A)) \leq n$. ■

## 2.2 Extension de Picard-Vessiot

### 2.2.1 Extension de Picard-Vessiot

**Lemme 2.2.1**

*Siot $R$ un anneau différentiel contenant $Q$*
*Si $I$ est un idéal différentiel de $R$ alors $\sqrt{I} = \{a \in R; \exists n \in \mathbb{N}^*, a^n \in I\}$ est un idéal différentiel de $R$.*

**Démonstration.**

Montrons que $\sqrt{I}$ est un idéal différentiel c-à-d $\forall a \in \sqrt{I},\ a^{'} \in \sqrt{I}$.
soit $a \in \sqrt{I}$ donc $\exists\ n \in \mathbb{N}^*; a^n \in I$, et comme $I$ est un idéal différentiel on a :

$$(a^n)^{'} \in I \Longrightarrow n(a^{n-1})a^{'} \in I$$

$$\Longrightarrow a^{n-1}a^{'} \in I \ldots\ (*)$$

On montre par récurrence que si : $\quad a^{n-k}(a^{'})^{2k-1} \in I \Longrightarrow a^{n-(k+1)}(a^{'})^{2(k+1)-1} \in I$

• Si $k = 0$ on a $(*)$

• Supposons que $a^{n-k}(a^{'})^{2k-1} \in I$ on a :

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

on multipliant par $a^{'}$ on a :

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

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

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

et donc

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

pour $n=k+1$ on a $(a^{'})^{2n-1}\in I$ donc $(a^{'})\in I$. ■

**Lemme 2.2.2**

*Siot $R$ un anneau différentiel simple contenant $Q$, alors $R$ est intégre et son corps de fractions a le même l'ensemble de constantes que $R$*

**Démonstration.**

• On a $I=\{0\}$ est un idéal diffirentiel de $R$ donc $\sqrt{I}=\{a\in R;\exists\ n\in\mathbb{N}^*:a^n=0\}$ est un idéal diffirentiel de $R$, et comme $R$ est simple et $1\notin\sqrt{I}$ alors $\sqrt{I}=\{0\}$ donc $R$ n'admet pas un élément nilpotent.

soient $a\in R$ et l'idéal $J_a=\{b\in R;\exists\ n\in\mathbb{N}^*,a^nb=0\}$, montrons que $J_a$ est un idéal diffirentiel de $R$

soit $b\in J_a$ donc $\exists\ n\in\mathbb{N}^*;\ a^nb=0\qquad(*)$

$$\begin{aligned}(*)\Longrightarrow(a^nb)^{'}=0&\Longrightarrow na^{n-1}a^{'}b+a^nb^{'}=0\\&\Longrightarrow a(na^{n-1}a^{'}b+a^nb^{'})=0\\&\Longrightarrow na^na^{'}b+a^{n+1}b^{'}=0\\&\Longrightarrow a^{n+1}b^{'}=0.\end{aligned}$$

donc $b^{'}\in J_a$

0n a $1\notin J_a$ car si $1\in J_a,\exists n\in\mathbb{N}^*;a^n=0$ absurde, donc $J_a\neq R$ et comme $R$ est simple $J_a=\{0\}$

soit $a,b\in R$ tels que $ab=0$ et $a\neq0$ donc $b\in J_a\Longrightarrow b=0$ donc $R$ est intégre .

• Soit $M$ le corps de fraction de $R$, on a $Const(R)\subset Const(M)$.

Soit $c$ une constante de $M$ donc $c^{'}=0$, et soit $J=\{a\in R; ac\in R\}$ on a :
$a\in J\Longrightarrow ac\in R\Longrightarrow (ac)^{'}\in R\Longrightarrow a'c+ac'\in R$

$$\Longrightarrow a'c\in R\Longrightarrow a'\in J$$

donc $J$ est un idéal différentiel de $R$.
et on a : $c\in M$ donc $c=\frac{p}{q}; p,q\in R$ et $q\neq 0$ donc $p=qc\in R$ donc $q\in J$ alors $J\neq\{0\}$, et $R$ est simple donc $J=R$

$$J=R\Longrightarrow 1\in J$$
$$\Longrightarrow 1.c\in R$$
$$\Longrightarrow c\in R$$

donc $Const(M)\subset Const(R)$ alors $Const(M)=Const(R)$. ■

**Lemme 2.2.3**

*Soit $(K,\delta)$ un corps différentiel de caractéristique nulle à corps de constantes $C$ algèbricmennt clos, soit $K\subset E$ une extension d'anneaux différentiel simple telle que $E$ est une $K-$algèbre de type fini, alors :*
*i) $Const(E)=C$*
*ii) si $M$ le corps de fraction de $E$, alors $Const(M)=C$*

**Démonstration.**

D'aprés le lemme précédent on a $Const(M)=Const(E)$ donc $Const(E)$ est un corps et $C\subset Const(E)$.
Pour montrer que $Const(E)\subset C$ il suffit de montrer que tout élément de $Const(E)$ est algébrique sur $K$.
car si $a\in Const(E)$ algébrique sur $K$ il existe $P=\lambda_0+\ldots+\lambda_{m-1}X^{m-1}+X^m; \lambda_i\in K; P(a)=0$.
on a

$$P(a)=0\Longrightarrow a^m+\lambda^{m-1}a_{m-1}+\ldots+\lambda_0=0$$
$$\Longrightarrow ma^{m-1}+((m-1)\lambda_{m-1}a^{m-2}a'+\lambda'_{m-1}a^{m-1})+\ldots+\lambda'_0=0$$
$$\Longrightarrow \lambda'_{m-1}a^{m-1}+\lambda'_{m-2}a^{m-2}+\ldots+\lambda'_0=0.$$

donc il existe $Q\in K[X]$ tel que $Q(a)=0$ avec $d^{\circ}Q\leq m-1<d^{\circ}P$ donc $Q=0$ donc $\lambda'_i=0$
donc $\lambda_i\in C$ alors $P\in C[X]$ donc $a$ algébrique sur $C$ et comme $C$ est algébriquement clos, $a\in C$ donc $C=Const(E)$. ■

**Définition 2.2.1**

*Soit $K \subset R$ une extension d'anneaux différentiels .On dit que $R$ est une extension de Picard-Vessiot d'anneaux associée au systeme $\Delta_A$ ssi :*

1) *Il existe une matrice fondamentale $U = (u_{i,j})_{1\leq i,j\leq n} \in GL(n, R)$ telle que :*

$R = K[u_{i,j}, \frac{1}{det(U)}];\ 1 \leq i, j \leq n.$

2) *$R = K[u_{i,j}, \frac{1}{det(U)}]$ est la plus ptite sous algébre de $R$ qui contient $K$ et $u_{i,j};\ \ 1 \leq i, j \leq n.$*

3) *$R$ est un anneau différentiel simple.*

**Définition 2.2.2**

*Soit $K \subset L$ une extension de corps différentiels. On dit que $L$ est une extension de Picard-Vessiot de corps associée au systeme $\Delta_A$ ssi :*

1) *Il existe une matrice fondamentale $U = (u_{i,j})_{1\leq i,j\leq n} \in GL(n, K)$ telle que :*

$L = K(u_{i,j});\ 1 \leq i, j \leq n.$

2) *$L = K(u_{i,j})$ est le plus petit sous corps de $L$ qui centient $K$ et $u_{i,j};\ \ 1 \leq i, j \leq n.$*

3) *$Const(L) = Const(K)$ .*

**Corollaire 2.2.4**

*Si $L$ est une extension de Picard-Vessiot d'anneaux ou corps associée au systéme $(\Delta_A)$. Alors $L$ est une extension de Picard-Vessiot associée au systeme $(\Delta_{Q_A})$.*

**Démonstration.**

Si $U = (u_{i,j})_{1\leq i,j\leq n}$ une matrice fondamentale du systéme $(\Delta_A)$ alors $QU$ est un matrice fondamentale de systéme $(\Delta_{Q_A})$.

si on pose $Q = (q_{i,j})_{1\leq i,j\leq n}$, alors $QA = (c_{i,j})_{1\leq i,j\leq n}$; $c_{i,j} = \sum_{k=1}^{n} q_{ik}.u_{kj}$ donc

$$K(c_{i,j}) = K\Big(\sum_{k=1}^{n} q_{ik}.u_{kj}\Big) = K(u_{k,j})$$

et

$$\begin{aligned} K\Big[c_{i,j}, \frac{1}{det(QU)}\Big] &= K\Big[\sum_{k=1}^{n} q_{ik}.u_{kj}, \frac{1}{det(U)}.\frac{1}{det(Q)}\Big] \\ &= K\Big[u_{kj}, \frac{1}{det(U)}\Big] \qquad 1 \leq j, k \leq n \end{aligned}$$

car $(q_{ik})_{1\leq i,k\leq n}$ , $\frac{1}{det(Q)} \in K$ ■

### 2.2.2 Proprietés des extensions de Picard-Vessiot

**Lemme 2.2.5**

*Soit $K \subset R$ extension de Picard-Vessiot d'anneaux associée à $(\Delta_A)$, alors $M$ le corps de fraction de $R$ est une extension de Picard-Vessiot de corps associée à $(\Delta_A)$.*

**Démonstration.**

Comme $K \subset R$ est une extension de Picard-Vessiot associée à $(\Delta_A)$ donc $R$ est simple, alors $R$ est intégre.

Si $U = (u_{i,j})_{1\leq i,j\leq n} \in GL(n, R)$ une matrice fondamentale du systéme $(\Delta_A)$ on a :

$R = K[u_{i,j}, \frac{1}{det(U)}]$ donc $M = K(u_{i,j})$

comme $R$ est une $K-$algébre de type fini donc $Const(R) = Const(K) = Const(M)$. ■

**Théorème 2.2.6**

*Soit $(K, \delta)$ un corps différentiel finie, $(\Delta_A)$ un système d'équations différencielles à coefficients dans $K$. Alors $(\Delta_A)$ admet une extension de Picard-Vessiot d'anneaux ou corps*

**Démonstration.**

Sioent $A = (a_{i,j})_{1\leq i,j\leq n}$ et l'anneau des polynômes $K[X_{i,j}; 1 \leq i, j \leq n]$ avec la dérivation qui étend celle de $K$ et vérifie :

$$X' = \sum_{k=1}^{n} a_{ik} X_{k,j}; \qquad 1 \leq i, j \leq n.$$

la dérivation du corps de fraction $K(X_{i,j})$ étend la dérivation de $K[X_{i,j}]$

on a $det(X_{i,j}) \neq 0$, on considére l'anneau différentiel $T = K[X_{i,j}, det(X_{i,j})] \subset K(X_{i,j})$.

Soit $\Sigma$ l'ensemble des idéaux différentiels de $T$ différents de $T$, on a $\{0\} \in \Sigma$.

Soit $(I_s)_{s\in S}$ une chaîne totalment ordonnée de $\Sigma$, alors $\bigcup_s I_s \in \Sigma$.

d'apré le lemme de Zorn il existe un idéal maximal $I$ différent de $T$ donc $R/I$ est un anneau différentiel simple.

Si $\overline{X}_{i,j} \in R$, $\overline{X}_{i,j} = X_{i,j} + I$, on a :

$$R = K\Big[\overline{X}_{i,j}, \frac{1}{\overline{X}_{i,j}}\Big].$$

on a :$(\overline{X}_{i,j})' = \overline{(X_{i,j})'} = A.\overline{(X_{i,j})'} = A(\overline{X}_{i,j})'$ donc $(\overline{X}_{i,j})_{i,j}$ est une matrice fondamentale de $(\Delta_A)$ donc $R$ est une extension de Picard-Vissiot d'anneaux associée à $(\Delta_A)$.

Si $M$ est le corps de fractions de $R$ alors $M$ est une extension de Picard-Vissiot de corps associée à $(\Delta_A)$. ■

**Théorème 2.2.7**

*Soient $K \subset R_1$ et $K \subset R_2$ deux extensions de Picard-Vissiot d'anneaux associées à $(\Delta_A)$. Alors il existe un isomorphisme d'anneaux différentiels $\sigma : R_1 \longrightarrow R_2; \sigma(k) = k$ si $k \in K$.*

**Démonstration.**

Soit $T = R_1 \otimes_K R_2$ qui est un anneau différentiel, comme $K$ est un corps, on peut considérer $R_1$ et $R_2$ comme $K-$espaces vectoriels non nuls donc $T \neq \{0\}$, alors il existe un idéal différentiel maximal $I$ de $T$ tel que $I \neq T$ donc $\overline{T} = T/I$ est un anneau différentiel simple.

On considére les homomorphismes différentiels :

$$j_1 : R_1 \longrightarrow \overline{T}$$

$$r_1 \longmapsto j_1(r_1) = r_1 \otimes 1 + I$$

et

$$j_2 : R_2 \longrightarrow \overline{T}$$

$$r_2 \longmapsto j_2(r_2) = 1 \otimes r_2 + I$$

Commme $1 \otimes 1 + I \neq \{\overline{0}\}$ donc $J_1, J_2$ sont non nuls.

Comme $R_1, R_2$ sont des anneaux différentiels simples et $ker(j_1), ker(j_2)$ sont des idéaux différentiels alors $ker(j_1) = \{0\}, ker(j_2) = \{0\}$ donc $j_1$ et $j_2$ sont injectifs.

En particulier $K \subset \overline{T}$

Sioent $U = (u_{i,j})_{1 \leq i,j \leq n}$ et $V = (v_{i,j})_{1 \leq i,j \leq n}$ deux matrices fondamentales de $(\Delta_A)$ telles que :

$$R_1 = K\left[u_{i,j}, \frac{1}{det(u_{i,j})}\right]$$

$$R_2 = K\left[v_{i,j}, \frac{1}{det(v_{i,j})}\right].$$

On note $\overline{u}_{i,j} = u_{i,j} \otimes 1 + I$ et $\overline{v}_{i,j} = 1 \otimes v_{i,j} + I$ et $\overline{U} = (\overline{u}_{i,j}), \overline{V} = (\overline{v}_{i,j})$ alors :

$$\overline{T} = K\left[\overline{u}_{i,j}, \overline{v}_{i,j}, \frac{1}{det(\overline{U})}, \frac{1}{det(\overline{V})}\right]$$

donc $\overline{T}$ est une $K$-algèbre de type fini et un anneau différentiel simple alors :

$Const(\overline{T}) = Const(K)$.

On a

$$j_1(R_1) = K\left[\overline{u}_{i,j}, \frac{1}{det(\overline{U})}\right] \subset \overline{T}$$

$$j_2(R_2) = K\Big[\overline{v}_{i,j}, \frac{1}{det(\overline{V})}\Big] \subset \overline{T}$$

On a $(\overline{U})' = \overline{U'} = \overline{A.U} = A.\overline{U}$ et $(\overline{V})' = \overline{V'} = \overline{A.V} = A.\overline{U}$ donc $(\overline{U})$ et $(\overline{V})$ sont des matrices fondamentales pour $(\Delta_A)$ alors il existe $C \in GL(n, Const(\overline{T})$ tel que $\overline{U} = C.\overline{V}$
Comme $Const(\overline{T}) \subset K$ $j_1(R_1) = j_2(R_2) = \overline{T}$ donc $j_1$ et $j_2$ surjectifs donc bijectifs, donc $j_1, j_2$ sont des isomorphismes différentiels, alors $j_2^{-1} \circ j_1$ est un isomorphisme différentiel qui laisse fixes les éléments de $K$. ■

**Théorème 2.2.8**

*Soient $K \subset L_1$ et $K \subset L_2$ deux extensions de Picard-Vissiot de corps associées au système $(\Delta_A)$. Alors il existe un isomorphisme de corps différentiels $\sigma : L_1 \longrightarrow L_2$, tel que $\sigma(k) = k$ si $k \in K$.*

**Démonstration.**

Soient $K \subset R$ l'extension de Picard-Vissiot d'anneaux construite dans le théoréme 2.2.6 et $L$ son corps de fractions.
Soit $K \subset M$ une extension de Picard-Vissiot de corps assocée au systéme $(\Delta_A)$.
On va montrer qu'il existe un homorphisme différentiel entre $L$ et $M$ qui laisse fixes les éléments de $K$.
Soient $U = (u_{i,j})$ et $V = (v_{i,j})$, matrices fondamentales pour $(\Delta_A)$, donc on a :

$$R = K\Big[u_{i,j}, \frac{1}{det(U)}\Big] \qquad et \qquad M = K(u_{i,j})$$

On considère $T = R \otimes_K M$, comme $K$ est un corps, $R$ et $M$ sont des $K$-espaces vectoriels non nuls . Alors $T \neq \{0\}$.
L'homomorphisme : $M \longrightarrow T;\ m \longmapsto 1 \otimes m$ injecte $M$ dans $T$. On a :

$$T = R \otimes_K M = M\Big[u_{i,j} \otimes 1, \frac{1}{det(U)} \otimes 1\Big].$$

Ainsi $T$ est une $M$-algébre de type fini.
Soit $I \neq T$ idéal différentiel maximal de $T$.
Soit $\overline{T} = T/I$, on considére les isomorphismes différentiels :

$$j_1 : R \longrightarrow \overline{T}$$

$$r \longmapsto j_1 = r \otimes 1 + I$$

et

$$j_2 : M \longrightarrow \overline{T}$$

$$m \longmapsto j_2 = 1 \otimes m + I$$

Comme $R$ est un anneau différentiel simple et $M$ est un corps différentiel donc $J_1$ et $J_2$ sont des homomorphismes différentiels injectifs donc $J_1$ et $J_2$ sont isomorphismes avec leurs images. En particulier $M \subset \overline{T}$ donc $\overline{T}$ est une $M$-algébre de type fini, Par ailleurs $\overline{T}$ est un anneau différéntiel simple. D'aprés le lemme 2.2.3 ona $Const(\overline{T}) = Const(M)$.
Comme $K \subset M$ est une extension de Picard-Vissiot de corps, on a $Const(K) = Const(M)$ donc $Const(\overline{T}) = Const(K)$.
On note $\overline{u}_{i,j} = u_{i,j} \otimes 1 + I$ et $\overline{v}_{i,j} = 1 \otimes v_{i,j} + I$ donc $\overline{U} = (\overline{u}_{i,j})$ et $\overline{V} = (\overline{v}_{i,j})$ sont des matrices fondamentales à cofficients dans $\overline{T}$
alors il existe une matrice $C \in GL(n, Const(\overline{T})$ telle que $\overline{U} = C.\overline{V}$. On a :

$$j_1(R) = K\Big[\overline{u}_{i,j}, \frac{1}{det(\overline{U})}\Big]$$

et

$$j_2(M) = K(\overline{v}_{i,j})$$

Comme $Const(\overline{T}) \subset K$ et $\overline{U} = C.\overline{V}$. on a $j_1(R) \subseteq j_2(M)$.
On considére l'homomorphisme différentiel $\sigma = j_2^{-1} \circ j_1 : R \longrightarrow M$ , on a $\sigma(k) = k,\ \forall\ k \in K$.
En particulier $\sigma$ non nul, Alors $\sigma$ est un homomorphisme différentiel car $R$ est simple .Alors $\sigma$ est s'étend sur le corps de fractions $L$ de $R$.
La matrice $(\sigma(u_{i,j}))$ est une matrice fondamentale pour $(\Delta_A)$ car $\sigma$ laisse fixes les éléments de $K$.
Alors il existe une matrice $C \in GL(n, Const(M))$ telle que $(\sigma(u_{i,j})) = C.V$. Comme $Const(K) = Const(M)$ on a :$\sigma(U.C^{-1}) = V$.
Ceci entraîne que $\sigma(L) = K(\sigma(u_{i,j})) = K(v_{i,j}) = M$.
Donc $\sigma$ est un isomorphisme différentiel entre $L$ et $M$ ■

**Corollaire 2.2.9**

*Soient $K \subset L$ une extension de Picard-Vissiot de corps associée $(\Delta_A)$, et $V = (v_{i,j})$ une matrice fondamentale pour $(\Delta_A)$ à coefficients dans $L$. On désigne par :*

$$R(L) = K\left[v_{i,j}, \frac{1}{det(V)}\right].$$

*Alors $R(L)$ ne dépend pas du choix de la matrice fondamentale $V$ et $R(L)$ est une extension de Picard-Vissiot d'anneaux associée $(\Delta_A)$.*
*En particulier $R(L)$ est un anneau différentiel simple.*

**Démonstration.**
Soit $W = (w)_{i,j}$ une autre matrice fondamentale pour $(\Delta_A)$ à coefficients dans $L$. Alors il existe une matrice $C \in GL(n, Const(L))$ telle que $W = C.V$. Comme $Const(L) = Const(K)$ on a :

$$K\Big[w_{i,j}, \frac{1}{det(W)}\Big] = K\Big[v_{i,j}, \frac{1}{det(V)}\Big] = R(L).$$

Soient $K \subset R$ un extension de Picard-Vessiot d'anneaux associée $(\Delta_A)$ et $M$ son corps de fractions. On a

$$R = K\Big[u_{i,j}, \frac{1}{det(U)}\Big].$$

Donc il existe un $K$-isomorphisme différentiel $\sigma : L \longrightarrow M$. Alors $(\sigma(u_{i,j}))$ est une matrice fondamental pour $(\Delta_A)$ à coefficients dans $L$. Donc

$$\sigma(R) = K\Big[\sigma(u_{i,j}), \frac{1}{det(U)}\Big] = R(L).$$

Alors $R$ et $R(L)$ sont $K$-isomorphes différentiablement, donc $R(L)$ est un extension de Picard-Vessiot d'anneaux .
En particulier $R(L)$ est un anneau différentiel simple. ∎

## 2.3 Groupe de Galois différentiel

Soit $(K, \delta)$ un corps différentiel de corps de constantes $C$ algébriquement clos de caracteristique nulle.
Soit $K \subseteq L$ une extension de Picard-Vessiot de $K$ pour le systéme différentiel $(\Delta_A)$

**Définition 2.3.1**
*Le groupe des $K$-automorphismes différentiels $\sigma : L \longrightarrow L$ fixant les éléments de $K$ et verifiant $\delta \circ \sigma = \sigma \circ \delta$ est appelé le groupe de Galois différentiel, noté par $Gal_K(L)$*

**Corollaire 2.3.1**
*Soient $\varphi \in Gal_K(L)$ et $f = (f_1, \ldots, f_n)^t \in Sol_L(\Delta_A)$ on a :*
*i) Si on désigne par $\varphi(f) = (\sigma(f_1), \ldots, \sigma(f_n))^t$ . Alors $\varphi(f) \in Sol_L(\Delta_A)$.*

*ii) L'application :*

$$\varphi : Sol_L(\Delta_A) \longrightarrow Sol_L(\Delta_A)$$
$$f \longmapsto \varphi(f)$$

*est un automorphisme du $C$-espace vectoriel $Sol_L(\Delta_A)$.*

**Démonstration.**

Soient $f = (f_1, \ldots, f_n)^t \in Sol_C(\Delta_A)$ et $\sigma \in Gal_K(L)$ on a :

$$\begin{aligned}(\varphi(f))' = (\sigma(f_1)', \ldots, \sigma(f_n)')^t &= (\sigma(f_1'), \ldots, \sigma(f_n'))^t \\ &= \varphi((f_1)', \ldots, (f_n)')^t) \\ &= \varphi(A.f) = A.\varphi(f).\end{aligned}$$

donc $\varphi(f) \in Sol_C(\Delta_A)$.

On définit l'application :

$$\varphi : Sol_C(\Delta_A) \longrightarrow Sol_C(\Delta_A)$$
$$f \longmapsto \varphi(f)$$

On montre que $\varphi$ est linéaire .

Soient $f = (f_1, \ldots, f_n)^t$ et $g = (g_1, \ldots, g_n)^t$

$$\begin{aligned}\varphi(f+g) &= \varphi(f_1 + g_1, \ldots, f_n + g_n) \\ &= (\sigma(f_1 + g_1), \ldots, \sigma(f_n + g_n))^t \\ &= (\sigma(f_1) + \sigma(g_1), \ldots, \sigma(f_n) + \sigma(g_n))^t \\ &= (\sigma(f_1), \ldots, \sigma(f_n))^t + (\sigma(g_1), \ldots, \sigma(g_n))^t \\ &= \varphi(f) + \varphi(g).\end{aligned}$$

Soient $\lambda \in C$ et $f = (f_1, \ldots, f_n)^t \in Sol_L(\Delta_A)$ on a :

$$\begin{aligned}\varphi(\lambda.f) = \varphi(\lambda f_1, \ldots, \lambda f_n) &= (\sigma(\lambda f_1), \ldots, \sigma(\lambda f_1)) \\ &= (\lambda.\sigma(f_1), \ldots, \lambda.\sigma(f_n)) \\ &= \lambda.\varphi(f).\end{aligned}$$

Comme $\sigma$ est bijictif et $\varphi(f) = (\sigma(f_1), \ldots, \sigma(f_n))^t$ donc $\varphi$ est bijictif. ■

**Proposition 2.3.2**

*Le groupe de Galois de $\Delta_A$ est isomorphe à un sous-groupe algébrique de $Gl(n, C)$.*

**Démonstration.**

On a le morphisme de groupes :

$$\rho : Gal_K(L) \longrightarrow Aut_C(Sol_C(\Delta_A))$$

$$\sigma \longmapsto \varphi$$

Soit $\sigma \in Gal_K(L)$ tel que : $\rho(\sigma) = id_{Sol_C(\Delta_A)}$

On a : $\varphi = id_{Sol_C(\Delta_A)} \Longrightarrow \forall f \in Sol_C(\Delta_A),\ \varphi(f) = f$

Soit $(F_1, F_2, \ldots, F_n)$ une base de $Sol_C(\Delta_A)$; $F_j = (f_{1,j}, \ldots, f_{n,j})$.

on a :

$$\varphi = id_{Sol_C(\Delta_A)} \Longrightarrow \varphi(F_j) = F_j$$

$$\Longrightarrow \sigma(f_{i,j}) = f_{i,j}\ ;\ \ 1 \leq i, j \leq n$$

Comme

$$\sigma : L \longrightarrow L \qquad et \qquad L = K(f_{i,j})$$

alors $\sigma = id_L$

Donc $\rho$ est injictif donc $Ker(\rho) = \{0\}$. On a

$$\frac{Gal_K(L)}{Ker(\rho)} \simeq Im\rho$$

et comme $Im\rho$ est un sous groupe de $Aut_C(Sol_C(\Delta_A)$ et $Aut_C(Sol_C(\Delta_A) \simeq Gl(n, C)$

Alors $Gal_K(L)$ est isomorphe à un sous groupe de $Gl(n, C)$. ■

**Remarque 2.3.1**

*Soit $H$ est un sous-groupe normal de $Gal_K(L)$. Alors le corps différentiel $F = L^H$ est normal sur $K$. En effet :*

*Le corps $L$ est normal sur $K$, donc il suffit de prouver que si $\sigma \in Gal_K(L)$, alors $\sigma(F) \subseteq F$.*

*Soient $a \in F$ et $\tau \in H$. Il existe $\varphi \in H$, tel que $\tau\sigma = \sigma\varphi$, car $H$ est normal.*

*On a $\tau\sigma(a) = \sigma\varphi(a) = \sigma(a)$, donc $\sigma(a) \in L^H = F$.*

*On a l'application*

$$Gal_K(L) \longrightarrow Gal_K(F)$$

$$\sigma \longmapsto \sigma_{/F}$$

*est surjective. Son noyau est* $G^F = Gal_F(L)$.

*On a donc l'isomorphisme de groupes*

$$\frac{Gal_K(L)}{Gal_F(L)} \simeq Gal_K(F).$$

**Exemple 2.3.1**

*Soit* $K \subset L$ *une extension de corps différentiels de caractiristique zéro. Soit* $t \in L$ *tel que* $t' \in K$ *et* $t'$ *n'est pas la dérevéé d'un élement de* $K$. *On a alors :*

(1) $t$ *est transcendant sur* $K$.

(2) *On a :* $Const(K(t)) = Const(K)$.

(3) *L'extension* $K(t)$*est une extension de Picard-Vissiot associeé à l'equation :*$y'' - \frac{a'}{a}y' = 0$.

(4) *Le groupe* $Gal_K(K(t))$ *isomorphe au groupe additif* $(Const(K), +)$.

*En effet :*

(1) *Supposons que* $t$ *est algébrique sur* $K$. *Soit* $P(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_0$ *le polynôme minimal de* $t$ *dans* $K$, *on a :*

$$\begin{aligned} P(t) = 0 &\Longrightarrow (P(t))' = 0 \\ &\Longrightarrow (mt' + a'_{m-1})t^{m-1} + \ldots + (a_1t' + a'_0) = 0 \\ &\Longrightarrow mt' + a'_{m-1} = 0 \\ &\Longrightarrow t' = -\frac{a'_{m-1}}{m}. \end{aligned}$$

*donc* $t'$ *est la dériveé de* $-\frac{1}{m}a_{m-1} \in K$ *en condradiction avec l'hypotése sur* $t'$ *donc* $t$ *est transcendant sur* $K$.

2) *Comme* $t^{'} \in K$ *donc* $K(t)$ *est un corps différentiel*

*On a* $Const(K[t]) = Const(K)$.

*Soit* $c = \frac{p(t)}{q(t)}$ *une constante de* $K(t)$ *avec* $p(t), q(t) \in K[t]$.

*On montrer par récurrence sur le degré* $d$ *de* $q$ *que* $c \in const(K)$.

*Si* $d = 0$ *alors* $c \in Const(K[t]) = Const(K)$ *sinon on suppposer que le coéfficient du terme de plus haut degré de* $q(t)$ *est* 1.

*Comme* $c^{'} = 0$, *On a :* $\quad c^{'} = 0 \Longrightarrow \frac{(p(t))'q(t) - p(t)(q(t))'}{q(t)^2} = 0$

$$\Longrightarrow \frac{(p(t))'q(t)}{q(t)^2} = \frac{p(t)(q(t))'}{q(t)^2}$$

$$\Longrightarrow \frac{(p(t))'}{((q(t))'} = \frac{p(t)}{q(t)} = c$$

*On applique l'hypothese de récurrence, donc* $c \in Const(K)$

(3) *Soit* $u_1 = 1$ *et* $u_2 = t$ *deux solutions linéarement indépendantes de l'equation différentielle linéaire* $y'' - \frac{a'}{a}y' = 0$ *on a :* $Const(K(t)) = Const(K)$ *et* $K(t,1) = K(t)$ *donc* $K \subset K(t)$ *est un extension de Picard-Vissiot de corps.*

(4) *Soit* $G = \left\{ M = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} ; M \in GL(2, Const(K)) \right\}$ *est un suos groupe de* $GL(n, Const(K))$

*l'application :*

$$G \longrightarrow (Const(K), +)$$

$$M \longmapsto c$$

*est un isomorphisme, donc* $Gal_K \simeq (Const(K), +)$

# Chapitre 3

# Extensions de Liouville

L'étude des extensions de Liouville, propriétés et existence fera l'objet de ce chapitre où on trouve un théorème fondamental d'existence de ce genre d'extensions liée fortement aux propriétés de la composante connexe de l'identité du groupe de Galois muni de la topologie de Zariski.

**Lemme 3.0.1**

*(i) Soient $K \subset L$ et $K \subset M$ deux extensions algébriques différentielles de corps, tout $K-$homomorphisme de corps $\delta : L \longrightarrow M$ est un homomorphisme de corps différentiels*

*(ii) Soit $K \subset L$ une extension de corps différentiel si $a \in L$ algébrique sur $K$ alors $K(a)$ est un corps différentiel.*

**Démonstration.**

*i*) Soient $a \in L$ algébrique et $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ le polynôme minimal de $a$ sur $K$.

on a : $P(a) = 0$ et $P(\delta(a)) = 0$. en dérivant ces deux égalités on obtient

$$a' = -\frac{P'(a)}{\frac{\partial P}{\partial X}(a)}$$

et

$$(\delta(a))' = -\frac{p'(\delta(a))}{\frac{\partial P}{\partial X}\delta(a)} \qquad (*)$$

où $P'(X) = a'_{n-1}X^{n-1} + \ldots + a'_0$. Alors

$$\delta(a') = -\delta\left(\frac{P'(a)}{\frac{\partial P}{\partial X}(a)}\right) = -\frac{P'(\delta(a)}{\frac{\partial P}{\partial X}(\delta(a))} = (\delta(a))'$$

donc $\delta$ est un homomorphisme différentil

*ii)* On a $a$ est algébrique sur $K$ donc $K \subset K(a)$ est un extension algébrique et d'apres $i)$ on a $K(a) \longrightarrow L$ est un homomorphisme différentiel donc $K(a)$ est un corps différentiel. ■

## 3.1 Extensions de Liouville

**Définition 3.1.1**

*Soit $K \subset L$ une extension de corps différentiel, on dira que l'extension $L$ est de type Liouvillien s'il existe une tour de corps différentiels $K = K_0 \subseteq K_1 \subseteq ... \subseteq K_m = L$ tel que :*
$\forall i = \overline{1,m}, K_i = K_{i-1}(t_i)$ *où* $t_i \in K_i$ *satisfait l'une des poprietés :*
(1) $t_i^{'} \in K_{i-1}$
(2) $\frac{t_i^{'}}{t_i} \in K_{i-1}$.
*Si $t_i$ est algebrique sur $K_{i-1}$ on dira que $L$ est de type Liouvillien généralisé.*

**Proposition 3.1.1**

*Soit $K \subset L$ extension de Picard-Vessiot à corps de constantes algébriquement clos et de caractéristique nulle.*
*Soient $\overline{K}$ le corps des éléments de $L$ algebriques sur $K$ et $G^0$ la composante connexe de l'identité de groupe $Gal_K(L)$,alors :*

$$\overline{K} = L^{G^0}$$

**Démonstration.**

D'aprés le lemme 1.1.23, $G^0$ est un sous-groupe normal et algébrique de $Gal_K(L)$. L'indice $[Gal_K(L) : G^0] = m$ est fini.
Soient $\sigma_1, \ldots, \sigma_m \in Gal_K(L)$, tels que

$$Gal_K(L)/G^0 = \{\sigma_1 G^0, \ldots, \sigma_m G^0 g\}$$

Soit $\sigma \in Gal_K(L)$, on a

$$\{\sigma_1 G^0, \ldots, \sigma_m G^0 g\} = \{\sigma\sigma_1 G^0, \ldots, \sigma\sigma_m G^0 g\}$$

Soit $F = L^{G^0}$. D'aprés la correspondance de Galois différentiel, on a $G^0 = Gal_K(L)^F$.
Soit $a \in F$, on considére le polynôme $P_a(X) = \Pi_{i=1}^m (X - \sigma(a))$.
Les éléments de $Gal_K(L)$ laissent fixes les coefficients de $P_a(X)$, donc $P_a(X) \in K[X]$. On a $P_a(a) = 0$. Donc $F \subset \overline{K}$.

Soit $a \in \overline{K}$. Soit $P(X)$ son polynôme minimal sur $F$. Soit $T = \{a_1, \ldots, a_t\}$ les racines de $P(X)$ dans $L$. D'aprés le lemme 3.0.1, le corps $M = F(a_1, \ldots, a_t)$ est diffèerentiel. Si $\sigma \in Gal_K(L)$, alors $\sigma(T) = T$, donc $\sigma(M) = M$. Alors l'extension $M$ est normal sur $F$, car l'extension $F \subset L$ est de Picard-Vessiot, donc normal. Soit $H = Gal_F(L)M$.
D'aprés la remarque 2.3.1, on a

$$Gal_F(M) \simeq \frac{Gal_F(L)}{Gal_M(L)} = \frac{G^0}{H}$$

Le groupe $Gal_F(M)$ est fini car il est contenu dans le groupe des permutations de $\{a_1, \ldots, a_s\}$. Le groupe $H$ est un sous-groupe normal linéaire et algébrique de $G^0$, et $G^0$ est un groupe linéaire algébrique connexe. Par le lemme 1.1.24 on a que $H = G^0$, donc $M = F, a \in F$, et $F = \overline{K}$. ■

**Corollaire 3.1.2**

*$K \subset L$ est de type Liouvillien si seulement s'il existe une tour de corps differentiels $K = M_0 \subset M_1 \subset ... \subset M_s = L$ tel que $\forall i = \overline{1, s}$, $M_i = M_{i-1}(z_i, w_i)$ où $z_i, w_i$ sont solutions différentes d'une équation differentielle linéaire de premiére ordre sur $M_{i-1}$*

$$y' + a_i y = b_i, \qquad\qquad a_i, b_i \in M_{i-1}.$$

**Démonstration.**

Si l'élément $t_i \in K_i$ vérifie $t_i' = b_i \in K_{i-1}$, on pose $z_i = t_i$ et $w_i = t_i + 1$ on a

$$K_i = K_{i-1}(t_i) = K_{i-1}(z_i, w_i) \;\; et \;\; z_i^{'} = t_i^{'} = b_i, \; w_i^{'} = (t_i + 1)^{'} = b_i.$$

si $t_i$ vérifie $t_i'/t_i = a \in K_{i-1}$, on pose $z_i = t_i$ et $w_i = 0$, qui sont solutions de l'équation $y' + a_i y = 0$.
réciproquement, soient $z$ et $w$ deux solutions différentes de l'équation $y' + a_i y = b_i$, où $a, b \in K$. Alors $u = z - w$ est une solution non nulle de l'équation homogéne $y' + ay = 0$. On a
$(z/v)' = b/v \in K(v)$. Soit $t_1 = v$ et $t_2 = z/v$. On a $K \subseteq K(t_1, t_2) = K(z, w)$ est une extension de type Liouvillien. ■

## 3.2 Extensions de Liouville et résolubilité

**Théorème 3.2.1**

*Soit $K \subset L$ une extension de corps différentiels telle que $L$ normal sur $K$ et $L = K(v_1, \ldots, v_m)$, l'extension $K \subset L$ est de type Liouvillien si pour tout $\sigma \in Gal_K(L)$ il exist $\lambda_{i,j}^{\sigma} \in Const(L)$ tels que :*

$$\sigma(v_i) = \lambda_{i,i}^{\sigma} v_i + \lambda_{i,i+1}^{\sigma} v_{i+1} + \ldots + \lambda_{i,m}^{\sigma} v_m;\ i = \overline{1,m} \qquad (*)$$

**Démonstration.**

On procéde par récurrence sur $m$.

Si $m = 0$ on a $K = L$ donc $L$ de type Liouvillien.

Pour $m \geq 0$, on divise $(*)$ par $\sigma(v_m) = \lambda_{m,m}^{\sigma}$ et on dérive, on a :

$$\sigma\Big(\Big(\frac{v_i}{v_m}\Big)'\Big) = \frac{\lambda_{i,i}^{\sigma}}{\lambda_{m,m}^{\sigma}}\Big(\frac{v_i}{v_m}\Big)' + \ldots + \frac{\lambda_{i,m-1}^{\sigma}}{\lambda_{m,m}^{\sigma}}\Big(\frac{v_{m-1}}{v_m}\Big)';\ \ i = 1, \ldots, m-1 \qquad (**)$$

Soit $M = K\Big(\Big(\frac{v_1}{v_m}\Big)', \ldots, \Big(\frac{v_{m-1}}{v_m}\Big)'\Big)$.

D'aprés $(**)$ ona $\forall \sigma \in Gal_K(L),\ \sigma(M) \subseteq M$.

On $K \subset M \subset L$ et comme $L$ est normal sur $K$ alors $M$ est normal sur $K$, donc $M$ est de type Liouvillien. D'aprés $(*)$ ona $\forall \sigma \in Gal_K(L),\ \sigma(v_m) = \lambda_{m,m}^{\sigma} v_m$

donc $\forall \sigma \in Gal_K(L),\ \sigma(\frac{v_m'}{v_m}) = \frac{v_m'}{v_m}$

comme $L$ est normal sur $K$ ,$\frac{v_m'}{v_m} \in M$ donc l'extension $M \subset M(v_m)$ est de type Liouvillien.

Comme $(\frac{v_i}{v_m})' \in M$, alors l'extension $M(v_m) \subset M(v_m)(\frac{v_1}{v_m}, \ldots, \frac{v_{m-1}}{v_m})$ est de type Liouvillien, donc $K \subset L$ est de type Liouvillien. ∎

**Théorème 3.2.2**

*Soient $K \subset L$ une extension de Picard-Vessiot à corps des constantes algébriquement clos et de caractéristique zéro, et $G^0$ la composante connexe de l'identité du groupe $Gal_K(L)$ Alors, si $G^0$ est résoluble, l'extension $K \subset L$ est de type Liouvillien généralisé.*

**Démonstration.**

Supposons que $G^0$ est résoluble, on a $K \subset L^{G^0}$ est une extension algébrique de type fini donc elle est de type Liouvillien généralisé.

On a $L^{G^0} \subset L$ est une extonsion de Picard-Vissiont et $G^0 = Gal_{L^{G^0}}(L)$ d'apré le théorème de Lie Kolchin il existe une base $\{\underline{v}_1, \ldots, \underline{v}_n\}$ de solutions du $\Delta_A$ tels que $\forall \sigma \in Gal_{L^{G^0}}(L)$, on a :

$$\sigma(\underline{v}_j) = \lambda_{j,1}^{\sigma}\underline{v}_1 + \ldots + \lambda_{j,n}^{\sigma}\underline{v}_n, \qquad \lambda_{j,k}^{\sigma} \in Const(K),\ 1 \leq j,k \leq n$$

on pose $\underline{v}_j = (v_{1,j}, \ldots, v_{n,j}) \in L^n$ si on ordonne les $v_{i,j},\ 1 \leq i, j \leq n$ donc le théorème 3.2.1 est satisfaite donc $K \subset L^{G^0} \subset L$ est de type Liouvillien, donc $L = K(\underline{v}_1, \ldots, \underline{v}_n)$ est de type Liouvillien généralisé. ■

**Théorème 3.2.3**

*Soient $K \subset L$ une extension de Picard-Vessiot à corps des constantes algébriquement clos et de caractéristique zéro, et $G^0$ la composante connexe de l'identité du groupe $Gal_K(L)$ . Si'l existe une extension de type Liouvillien généralisé $K \subset F$ telle que $L \subset F$ et $Const(F) = Const(K)$, alors $G^0$ est résoluble.*

**Démonstration.**

On montrer par récurrence sur la longueur de la tour $K = F_0 \subset F_1 \subset \ldots \subset F_m = F$

Si $m = 0$ ona $K = F$ donc $G^0 = id_K$ est résoluble.

Soit $\overline{K}$ le corps des élément de $L$ algébrique sur $K$ donc $\overline{K} = L^{G^0}$ donc $Gal_{\overline{K}}(L) = G^0$

supposont que $\overline{K} = K$, On a $\overline{K} \subset \overline{K}(t_1) \subset \ldots \subset \overline{K}(t_1, \ldots, t_m) = F$ définit un extension de type Liouvillien généralisé $\overline{K} \subset F$.

Soit $U \in GL(n, L)$ une matrice fondamentale de $(\Delta_A)$, commme $Canst(F) = canst(K)$ ona $K(t_1) \subset L(t_1)$ est une extension de Picard- Vessiot assosié à $\Delta_A$ et $V \in GL(nL(t_1))$ est une matrice fondamentale de $(\Delta_A)$.

Ona

$$P : Gal_{K(t_1)}(L(t_1)) \longrightarrow Gal_K(L)$$

$$\sigma \longmapsto \sigma_{/L}$$

est un homomorphisme de groupes algépriques.

Soit $H = Gal_{K(t_1)}(L(t_1))$ on a $H \in Gal_K(L)$

ona $L^H = L \cap K(t_1)$ car si $a \in L \backslash (L \cap K(t_1)),\ \exists \sigma \in H;\ \sigma(a) \neq a$

Comme $\overline{K}(t_1) \subset \ldots \subset \overline{K}(t_1, \ldots, t_m) = F$ de longuer $(m-1)$ donc d'aprés l'hypothés de récurense $H^0$ de $H$ est résoluble.

Supposont que $t_1$ est algébrique sur $K$ donc $K(t_1)$ algébrique et comme $K = \overline{K}$

donc $K = L \cap K(t_1)$ donc $L^H = K$

on a $H = Gal_K(L)$ donc $Gal_K(L) = G^0 = H^0$ est résoluble. ■

# Bibliographie


[1] Y. André . *Solution algebras of differential equations and quasi-homogeneous varieties a new differential Galois correspondance,* Ann-sci-ecole norm.sup, 47(2), 2014.

[2] N. Bourbaki. *Algèbre commutative*, Masson, chapitre 3, 1985.

[3] J. Cano et J. P. Ramis. *Théorie de Galois différentielle, multisommabilité et phénoménes de stokes.*

[4] K. Conrad. *Decomposing* $SL_2(\mathbb{R})$.

[5] B. Deschamps. *Théorie de Galois*, Saint-Etienne, 2002/2003.

[6] I. Kaplansky. *Différential algebra* , Herenann, 1976.

[7] S. Krioui. *Groupe de Galois différentiel,*Mémoire de Master, Université de JIJEL, 2015-2016.

[8] E. R. Kolchin. *Différential algebra and algebraic groups,* Volume 54 of Pur and Applied Mathématics, Academic Presse, 1973.

[9] Jerald J. Kovacic. *Algorithm for solving second order linear homogenoeus différential équation* , Journal of symbolic computation, 1986.

[10] Andy R. Magid. *Lectures on différential Galois théory* , Volume 7 of university lectur series, American Mathématical socity, 1994.

[11] F. Ronga .*Notes de géométrie algébrique.*

[12] Michael.F. Singer. *An outline of différential Galois théory. In evelyne tournier, editor, computer algebra and différential équations,* Academic Presse, 1989

[13] Michael.F. Singer and felix ulmer . *Liouvillian and algebric solutions of second and third order linear differential équations*, Journal of symbolic computation, 1993.

[14] Michael.F. Singer. *Liouvillian solutions of* $n^{th}$ *order homogenoeus linear differetial équations ,* American journal of mathematics, 103-661-682, 1981.

[15] M. Vamder and M. Fasinger. *Galois theory of linear differential equations.* Volume 328 of grundlehren des mathematischen issenschalfeten(fondamental principles of mathematical sciences), Springer verlag, Berlin, 2003.

[16] M. Vanderput. *Galois theory of differential equations, algebraic groupes and Lie algebras*, Journal of symbolic computation, 1999.