Théorie des corps et applications

Royer Lucas

15 mai 2024

Table des matières

0.1 Introduction

Au sein de ce mémoire de recherche nous allons explorer les concepts fondamentaux en algèbre, d'extensions de corps et de théorie de Galois. Nous verrons comment ces méthodes introduites au cours du XIX siècle, ont permis d'apporter un éclairage nouveau à de nombreux domaines des mathématiques, comme la théories des équations, la géométrie et les algèbres de fonctions.

Le fil rouge de ce mémoire sera de démontrer des résultats classiques d'impossibilités dans des domaines mentionnés ci-dessus.

0.2 Théorie et extensions de corps

L'objet fondamental que nous allons étudier tout au long de ce mémoire, est celui d'extension de corps. Sauf mention contraire dans tout le mémoire nous désignerons par corps un corps commutatif.

0.2.1 Extensions de corps

Définition 1 (Extension de corps)**.** Soit k un corps, on dit que le couple (K, j) est une extension du corps k si K est un corps et j un homomorphisme d'anneau de k dans K.

Remarque 2. Avec les notations précédentes on a $ker(j) \neq k$, car $j(1_k) = 1_k$. Or, $ker(j)$ est un idéal de k, donc il est égal à k ou $\{0\}$. Il vient que j est injectif, on peut donc identifier k avec son image $j(k)$ dans K. En pratique on fera cette identification, et on dira que K est une extension de k si k est un sous-corps de K. On notera $k \subset K$.

Définition 3 (degré d'une extension)**.** Soit $k \subset K$ une extension de corps. Alors K est un k-espace vectoriel. Le cardinal d'une base de K vu comme k-espace vectoriel est appelé le degré de l'extension, et est noté $[K : k]$.

Définition 4 (nombre algébrique et transcendant)**.** Soit $k \subset K$ une extension de corps et $x \in K$. Considérons l'application suivante :

$$\Phi_x : k[X] \to K$$
$$P \mapsto P(x)$$

Cette application est un homomorphisme de k-algèbre d'image $k[x]$. Si l'on note $\mathfrak{a}_x$ son noyau, deux cas sont possibles :

$\mathfrak{a}_x = \{0\}$. On dit dans ce cas que x est transcendant sur k.

$\mathfrak{a}_x \neq \{0\}$. On dit dans ce cas que x est algébrique sur k.

Définition 5. Soit $k \subset K$ une extension de corps. On dit que K est une extension algébrique si tous ses éléments sont algébriques sur k. Si elle n'est pas algébrique on dit qu'elle est transcendante.

Définition 6. On dit d'un corps K qu'il est algébriquement clos si tout élément de $K[X] \setminus K$ admet au moins une racine dans K.

0.2.2 Extensions de décomposition

Définition 7. Soient $k \subset K$ et $k \subset L$ deux extensions d'un même corps k. On appelle un k-homomorphisme de K dans L tout homomorphisme σ du corps K dans L tel que $\sigma(x) = x$ pour tout $x \in k$. On note $Hom_k(K, L)$ l'ensemble des k-homomorphismes de K dans L.

Définition 8. Soit $k \subset K$ une extension. Le groupe $Isom_k(K, K)$ (groupe des k-automorphismes) est appelé le groupe de Galois de K sur k. Il est noté $Gal(K \setminus k)$.

Définition 9. Soit $F = (P_i)_{i \in I}$ une famille de polynômes non constants de $k[X]$. On appelle corps de décomposition, ou extension de décomposition de la famille F toute extension K de k qui vérifie les propriétés suivantes :

1) Pour tout $i \in I$, le polynôme P_i est scindé sur K. Soit R_i l'ensemble des racines de P_i dans K.

2) Si R est la réunion des R_i, alors on a $K = k(R)$.

Proposition 10. Soient $k \subset K$ une extension et $\mathcal{A}$ une k-algèbre. On note $\mathcal{H}$ l'ensemble des homomorphismes de k-algèbres de $\mathcal{A}$ dans K. Alors, $\mathcal{H}$ est une partie libre de $L_k(\mathcal{A}, K)$, l'espace vectoriel des applications linéaires de $\mathcal{A}$ dans K.

Démonstration. Soit $u_,..., u_n$ une suite d'élément deux à deux distincts de $\mathcal{H}$. Montrons le résultat par récurrence sur n. Si $n = 1$ c'est clair puisque l'on a des applications linaires donc en particulier non nulles.

Soient $\lambda_1, ..., \lambda_n \in K$ et tels que $\lambda_1 u_1 + ... + \lambda_n u_n = 0$. Si $x, y \in \mathcal{A}$, on a :

$$\sum_{i=1}^{n-1} \lambda_i (u_i(x) - u_n(x)) u_i(y) = \sum_{i=1}^{n} \lambda_i u_i(xy) - u_n(x) \sum_{i=1}^{n} \lambda_i u_i(y) = 0$$

On en déduit que pour tout $x \in \mathcal{A}$:

$$\sum_{i=1}^{n-1} \lambda_i(u_i(x) - u_n(x))u_i = 0$$

Or d'après les hypothèses de récurrences, on obtient $\lambda_i(u_i(x) - u_n(x)) = 0$ pour tout $1 \leq i \leq n-1$ et pour tout $x \in \mathcal{A}$. Les u_i étant distincts, il vient $\lambda_i = 0$ si i est distinct de n. Enfin $\lambda_n u_n = 0$ et $\lambda_n = 0$ puisque $u_n \neq 0$. □

Corollaire 11 (Théorème de Dedekind)**.** Soient $k \subset K$ et $k \subset L$ des extensions de k.

— Le sous ensemble $Hom_k(K, L)$ est libre sur L.

— Si l'extension $k \subset K$ est finie, on a :

$$\text{card } Hom_k(K, L) \leq [K : k] \text{ et card } Gal(K \setminus k) \leq [K : k]$$

Démonstration. La première assertion est claire d'après la proposition précédente. Pour prouver la seconde il suffit d'établir la première inégalité. Posons $n = (K : k]$, et soit $(e_1, ..., e_n)$ une base du k-espace vectoriel K.

Supposons qu'il existe $\sigma_1, ..., \sigma_{n+1} \in Hom_k(K, L)$ distincts deux à deux. Soit la matrice $M \in M_{n,n+1}(L)$ définit par $(M)_{ij} = \sigma_j(e_i)$. Le rang de M est au plus n. Par conséquent si $C_1, ..., C_{n+1}$ sont les colonnes de M, il existe $\lambda_1, ..., \lambda_{n+1} \in L$ non tous nuls tels que :

$$\lambda_1 C_1 + ... + \lambda_{n+1} C_{n+1} = 0$$

Donc pour tout $i \in [\![1, n]\!]$,

$$\lambda_1 \sigma_1(e_i) + ... + \lambda_{n+1} \sigma_{n+1}(e_i) = 0$$

L'application k-linéaire $\lambda_1\sigma_1 + ... + \lambda_{n+1}\sigma_{n+1}$ de K dans L s'annule sur une base de K. Elle est donc nulle. Ainsi $\sigma_1, ..., \sigma_{n+1}$ sont lié sur L ce qui contredit la proposition précédente. □

Lemme 12. Pour $i = 1, 2$, soit $k_i \subset K_i$ une extension, a_i un élément de K_i, algébrique sur k_i. Notons P_i son polynôme minimal sur k_i. On suppose qu'il existe un isomorphisme σ de k_1 sur k_2 et tel que $\bar{\sigma}(P_1) = P_2$. Ici $\bar{\sigma}$ prolonge σ sur les anneaux de polynômes correspondants. Il existe alors un unique isomorphisme θ de $k_1(a_1)$ sur $k_2(a_2)$ prolongeant σ, et tel que $\theta(a_1) = a_2$.

Démonstration. L'isomorphisme $\bar{\sigma}$ induit par passage au quotient, un isomorphisme $\tilde{\sigma}$ de $k_1[X] \setminus (P_1)$ sur $k_2[X] \setminus (P_2)$. Par ailleurs les applications :

$$k_1[X] \to K_1, P \mapsto P(a_1) \text{ et } k_2[X] \to K_2, P \mapsto P(a_2)$$

induisent les isomorphismes :

$$f_1 : k_1[X] \setminus (P_1) \to k_1(a_1) \text{ et } f_2 : k_2[X] \setminus (P_2) \to k_2(a_2)$$

Il est immédiat que $\theta = f_2 \circ \tilde{\sigma} \circ f_1^{-1}$ vérifie les conditions du lemme. L'unicité provient du fait que a_i engendre $k_i(a_i)$. □

Théorème 13. Soient $k \subset K$ une extension algébrique et Ω un corps algébriquement clos. Soit σ un homomorphisme de k dans Ω.

- Il existe un homomorphisme θ de K dans Ω prolongeant σ.
- On suppose que K est algébriquement clos et que $\sigma(k) \subset \Omega$ est une extension algébrique. Tout homomorphisme de K dans Ω prolongeant σ est en fait un isomorphisme.

Démonstration. La preuve qui va suivre nécessite l'axiome du choix, par l'intermédiaire du lemme de Zorn qui lui est équivalent.

Montrons le premier point. Soit $\mathcal{E}$ l'ensemble des couples (L, ϕ), où L est un sous corps de K contenant k, et ϕ un homomorphisme de L dans Ω qui prolonge σ. On a $(k, \sigma) \in \mathcal{E}$. On peut ordonner $\mathcal{E}$ de la façon suivante :

$$(L, \phi) \leq (M, \psi) \Leftrightarrow L \subset M \text{ et } \psi | L = \phi$$

Munit de cet ordre il est immédiat que $\mathcal{E}$ est inductif. Le lemme de Zorn permet alors d'affirmer que $\mathcal{E}$ possède un élément maximal (L, θ). Prouvons que $L = K$.

Supposons que $L \neq K$, et soit $a \in K \setminus L$. On note P le polynôme minimal de a sur L, et $Q = \bar{\theta}(P)$ (on reprend les mêmes notations que dans le lemme précédent). Le corps Ω étant algébriquement clos, il existe $b \in \Omega$ tel que $Q(b) = 0$. D'après le lemme précédent, θ se prolonge en un homomorphisme ϕ de $L(a)$ dans Ω et tel que $\phi(a) = b$. On obtient une contradiction sur le caractère maximal de (L, θ). Ceci conclut la preuve du point 1.

Montrons maintenant le second point. Si l'extension $\sigma(k) \subset \Omega$ est supposé algébrique, il en est de même pour l'extension $\theta(K) \subset \Omega$. En outre, si K est algébriquement clos, $\theta(K)$ l'est également. On a donc $\theta(K) = \Omega$. □

Théorème 14 (Steiniz)**.** Tout corps k possède une extension algébriquement close.

Démonstration. Soit $\mathcal{P}$ l'ensemble des éléments non constants de $k[X]$, et soit $(X_P)_{P\in\mathcal{P}}$ une famile d'indéterminées sur k. On note $\mathfrak{a}$ l'idéal de l'anneau $\mathcal{A} = k[(X_P)_{P\in\mathcal{P}}]$ engendré par les polynômes $P(X_P)$, avec $P \in \mathcal{P}$.

Supposons que $\mathcal{A} = \mathfrak{a}$. Il existe alors un entier $n \in \mathbb{N}^*$, $Q_1, ..., Q_n \in \mathcal{A}$, et des éléments $P_1, ..., P_n \in \mathcal{P}$ tels que :

$$Q_1P_1(X_{P_1}) + ... + Q_nP_n(X_{P_n}) = 1$$

Montrons qu'il existe une extension K de k telle que chacun des P_i possède une racine a_i. Sans pertes de généralités les P_i sont irréductible. Si $n = 1$ alors le corps $k[X]/(P(X))$(on quotiente par l'idéal engendré par P) fonctionne. Sinon par récurrence supposons qu'il existe une extension finie $k \subset L$ tel que $P_1, ..., P_{n-1}$ aient une racine dans L. Soit Q un facteur irréductible de P_n dans $L[X]$. On a alors le résultat en prenant pour K le corps Ł$[X]/(Q(X))$.

En substituant a_i à X_{P_i}, si $1 \leq i \leq n$ et 0 à X_P si $P \notin \{P1, ..., P_n\}$, on obtient $0 = 1$, ce qui est évidement une contradiction.

D'après ce qui précède, $\mathfrak{a}$ est contenu dans un idéal maximal $\mathfrak{m}$ de $\mathcal{A}$(l'existence de cet idéal est assuré par le théorème de Krull, on pourra par exemple consulter [7]). De plus $K_1 = \mathcal{A}/\mathfrak{m}$ est un corps. Soit $\sigma : \mathcal{A} \to K_1$, la surjection canonique. Comme $1 \notin \mathfrak{m}$, la restriction $\sigma|k$ est injective. On peut donc dire que k s'identifie à un sous-corps de K_1.

Si $P \in \mathcal{P}$ et si $\xi_P = \sigma(X_P)$, on a alors $P(\xi_P) = 0$, car $P(X_P) \in \mathfrak{m}$. Par conséquent, tout élément de $\mathcal{P}$ a une racine dans K_1.

En itérant ce procédé, on peut construire une suite de corps :

$$k \subset K_1 \subset ...K_n \subset ...$$

telle que tout élément de $K_n[X] \setminus K_n$ ait une racine dans K_{n+1}. Soit K la réunion des K_n. Alors K est un corps. Si $P \in K[X]$ est non constant, il appartient à un anneau $K_n[X]$, et admet donc une racine dans $K_{n+1} \subset K$. Le corps K est donc algébriquement clos. □

Définition 15. Une extension K de k est appelée clôture algébrique de k si elle est algébriquement close et algébrique sur k.

0.2.3 Extensions séparables

Proposition 16. Soient $P \in k[X]$ de degré $m \geq 1$ et Ω une extension algébriquement close de k. Les conditions suivantes sont équivalentes :

1) Les polynômes P et P' sont premiers entre eux dans $k[X]$.

2) Pour toute extension K de k, les polynômes P et P' sont premiers entre eux dans $K[X]$.

3) Pour toute extension K de k, les polynômes P et P' sont sans racines communes dans K.

4) Il existe une extension K de k telle que P se décompose dans $K[X]$ en produit de polynômes non associés (i.e P divise Q et Q divise P) de degré 1.

5)Les racines de P dans Ω sont simples.

6)P n'a que des racines simples dans toute extension K de k.

Démonstration. 1)$\Leftrightarrow$ 2) : C'est clair d'après l'algorithme d'Euclide.

3)$\Leftrightarrow$ 6) : Cela découle directement du fait qu'une racine d'un polynôme est simple si et seulement si elle n'est pas racine du polynôme dérivé.

1)$\Rightarrow$ 5) : Si 1) est vérifié alors par le théorème de Bezout, il existe $U, V \in k[X]$ tel que $PU + P'V = 1$. Si $a \in \Omega$ est racine de P, on a alors $P'(a)V(a) = 1$, et donc $P'(a) \neq 0$, et a est racine simple de P.

5)$\Rightarrow$ 4) : c'est évident.

4)$\Rightarrow$ 1) : Si 4) est vrai, les polynômes P et P' sont premiers entre eux dans $K[X]$, et donc dans $k[X]$.

2)$\Rightarrow$ 3) : Si $a \in K$ est racine commune à P et P', alors $X - a$ divise P et P'.

3)$\Rightarrow$ 5) La condition 3) implique que toutes les racines de P dans Ω sont simples pour les mêmes raisons que dans la seconde équivalence.

□

Définition 17. On dit que $P \in k[X]\backslash k$ est séparable s'il vérifie les conditions équivalentes de la proposition précédente.

Lemme 18. Soit $P \in k[X]$ tel que $P' = 0$.

1) Si $car(k) = 0$, alors P est constant.

2) Si $car(k) = p > 0$, alors il existe alors $Q \in k[X]$ tel que $P(X) = Q(X^p)$.

Démonstration. On a :

$$P(X) = \sum_{i=0}^{n} a_i X^i \Rightarrow P'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$$

Ainsi, $P' = 0$ si et seulement si $ia_i = 0$, pour $1 \leq i \leq n$. Le résultat est donc clair si $car(k) = 0$. Si $car(k) = p > 0$, cela signifie que i est multiple de p dès que $a_i \neq 0$. D'où l'assertion. □

Proposition 19. Soit P un élément irréductible de $k[X]$. Les conditions suivantes sont équivalentes.

1) Le polynôme P est séparable.

2) Il existe une extension K de k dans laquelle P a une racine simple.

3) $P' \neq 0$.

4) Ou bien le corps est de caractéristique nulle, ou bien il est de caractéristique p et $P \notin k[X^p]$.

Démonstration. 1) $\Rightarrow$ 2) Il suffit de prendre pour K une clôture algébrique de k.

2) $\Rightarrow$ 3) Si a est une racine simple du polynôme P dans une extension de k, on a alors $P'(a) \neq 0$ et donc $P' \neq 0$.

3) $\Leftrightarrow$ 4) Cela résulte du lemme précédent.

3) $\Rightarrow$ 1) Soit Ω une extension algébriquement close de k, et soit x une racine de P dans Ω. Comme P est irréductible, P est le polynôme minimal de x sur k. De $\deg(P') < \deg(P)$ et $P' \neq 0$, on déduit que $P'(x) \neq 0$. Par suite, x est racine simple de P, et on vérifie le point 1).

□

Définition 20. Soit $k \subset K$ une extension, et $a \in K$.

1) On dit que a est séparable sur k s'il est algébrique et si son polynôme minimal sur k est séparable.

2) Une extension $k \subset K$ est dite séparable si elle est algébrique et si tout élément de K est séparable sur k.

Définition 21. L'extension $k \subset K$ est dite de type fini (respectivement simple) s'il existe une partie finie S de K (respectivement une partie ne contenant qu'un seul élément) et telle que $K = k(S)$. Dans le cas où l'extension est simple, un élément x tel que $K = k(x)$ est appelé élément primitif de l'extension.

Lemme 22. Soient Ω une extensions algébriquement close de k, et $x \in \Omega$. On suppose x algébrique et séparable sur k, de degré n. Pour tout homomorphisme σ de k dans Ω, il existe exactement n homomorphismes de $k(x)$ dans Ω prolongeant σ.

Démonstration. Soit P le polynôme minimal de x sur k. P possède n racines distinctes dans Ω. Il en est donc de même pour $\bar{\sigma}(P)$, cette notation désignant l'application de σ aux coefficients de P. Notons $x_1, ..., x_n$ les racines de $\bar{\sigma}(P)$ dans Ω. Il existe un isomorphisme (lemme 12) $\tau_i : k(x) \to \sigma(k)(x_i)$, pour $1 \leq i \leq n$. Ils prolongent σ et sont tels que $\tau_i(x) = x_i$. Les τ_i se prolongent en des homomorphismes $\sigma_i : k(x) \to \Omega$(théorème 13). Ils sont distincts, car $\sigma_i(x) = x_i$.

Enfin soit $\eta : k(x) \to \Omega$ un homomorphisme prolongeant σ. Alors $\eta(x)$ est racine de $\bar{\eta}(P) = \bar{\sigma}(P)$, et donc $\eta(x) = \tau_l$, pour $1 \leq l \leq n$. Or η prolongeant σ, est entièrement déterminé par $\eta(x)$. D'où $\eta = \tau_l$. □

Proposition 23. Soient Ω une extension algébriquement close de k et K une extension séparable de degré fini n de k. Alors card $Hom_k(K, \Omega) = n$.

Démonstration. Si $n = 1$, le résultat est clair. De même si l'extension $k \subset K$ est simple, il résulte du lemme précédent que $\sigma = id_k$. On suppose donc que $n \geq 2$ et que K n'est pas une extension finie de k. Il existe alors un corps L et un élément de K tel que $k \subsetneq L \subsetneq K$ et $K = L(x)$. Les extensions $k \subset L$ et $L \subset K$ sont séparables.

Posons $r = [L : k]$ et $s = [K : L]$. On a $r \leq n$. Si l'on raisonne par récurrence sur n, on a card $Hom_k(L, \Omega) = r$. Notons $\sigma_1, ..., \sigma_r$ les éléments de cet ensemble. D'après le lemme précédent, chacun des σ_i se prolonge en exactement s éléments distincts de $Hom_k(K, \Omega)$. D'où card $Hom_k(K, \Omega) \geq rs = n$.

Soit $\sigma \in Hom_k(K, \Omega)$. Alors, $\theta = \sigma|L$ est l'un des σ_i. Comme σ est déterminé par θ et $\sigma(x)$, σ est l'un des élément de $Hom_k(K, \Omega)$ obtenus précédemment. □

Lemme 24. Soient E un k-espace vectoriel, $n \in \mathbb{N}^*$, et $E_1, ..., E_n$ des sous espaces de E distincts de E. Si card $k \geq n$ on a $E \nsubseteq E_1 \cup ... \cup E_n$.

Démonstration. On pose $F_i = E_1 \cup ... \cup E_i$ avec $1 \leq i \leq n$. Le résultat est clair si $i = 1$. On va le prouver par récurrence sur n en supposant donc $n \geq 2$.

Supposons $F_n = E$ et card $k \geq n$. D'après l'hypothèse de récurrence, on a $F_{n-1} \neq E$. Il existe donc un $x \in E_n \setminus F_{n-1}$. Enfin fixons $y \in E \setminus E_n$.

Considérons l'application $u : k \to E$, $\lambda \to \lambda x + y$. Comme $x \in E_n$, $y \notin E_n$, on a $u(\lambda) \notin E_n$, et cela pour tout $\lambda \in k$, d'où $u(k) \subset F_{n-1}$. Puisque card $k \geq n$, il existe $l \in [\![1; n-1]\!]$, et $\lambda, \mu \in k$ vérifiant $\lambda \neq \mu$ et $u(\lambda), u(\mu) \in E_l$. Alors on a :

$$x = (\lambda - \mu)^{-1}(u(\lambda) - u(\mu)) \in E_l$$

Contradiction. □

Théorème 25 (Théorème de l'élément primitif)**.** Une extension $k \subset k$ séparable et de degré fini possède un élément primitif.

Démonstration. Si k est un corps fini, alors K est fini, et donc le groupe multiplicatif K^* est cyclique. Si x est un générateur de ce groupe, il est clair que $K = k(x)$. Supposons donc k infini. Soit Ω une clôture algébrique de K et donc de k. Si $n = [K : k]$, on note $\sigma_1, ..., \sigma_n$, les éléments de $Hom_k(K, \Omega)$ (proposition 23). Pour $i, j \in \mathbb{N}^*$ distincts, posons :

$$E_{i,j} = \{x \in K; \sigma_i(x) = \sigma_j(x)\}$$

Il est immédiat que $E_{i,j}$ est un k-sous-espace vectoriel de K mais distinct de lui même puisque $\sigma_i \neq \sigma_j$.

D'après le lemme précédent, il existe $x \in K$ tel que $\sigma_i(x) \neq \sigma_j(x)$, pour tous $i, j \in \mathbb{N}^*$, et distincts. Par suite $n \leq$card $Hom_k(K, \Omega)$, et donc $n \leq [k(x) : k]$ d'après le théorème de Dedekind. L'inégalité opposée étant claire, on a $[k(x) : k] = 1$ et $K = k(x)$, et donc x est un élément primitif de $k \subset K$. □

0.2.4 Extensions normales

Dans la suite de cette section on note $\tilde{k}$ une clôture algébrique de k.

Définition 26. Une extension $k \subset K$ est dite normale si elle est algébrique et si tout polynôme irréductible de $k[X]$ ayant au moins une racine dans K, est produit dans $K[X]$ de polynôme de degré 1(on dira que le polynôme est scindé).

Lemme 27. Soient $k \subset K \subset \tilde{k}$ des extensions, et soit $\sigma \in Hom_k(K, \tilde{k})$.
- Si $\sigma(K) \subset K$, alors σ induit un élément de $Gal(K \setminus k)$.
- Il existe $\tau \in Gal(\tilde{k} \setminus k)$ prolongeant σ.

Démonstration. Pour le premier point. Soit $x \in K$, et soit P son polynôme minimal sur k. On note S l'ensemble des racines de P dans K. L'ensemble S est fini, σ est une injection de K dans K et $\sigma(S) \subset S$. D'où $\sigma(S) = S$. Comme $x \in S$ il vient $x \in \sigma(K)$. Ainsi $\sigma(K) = K$. L'assertion en résulte.

Pour le second point, il est clair que $\tilde{k}$ est une clôture algébrique de K et de $\sigma(K)$. Le résultat est alors une conséquence du théorème 13. □

Définition 28.
- On dit que des éléments x, y de $\tilde{k}$ sont conjugués s'il existe $\sigma \in Gal(\tilde{k} \setminus k)$ tel que $\sigma(x) = y$.
- Deux extensions K et L de k contenues dans $\tilde{k}$ sont dites conjuguées s'il existe $\sigma \in Gal(\tilde{k} \setminus k)$ tel que $\sigma(K) = L$.

Théorème 29. Si $x, y \in \tilde{k}$ les conditions suivantes sont équivalentes :

1) x et y sont conjugués sur k.
2) Il existe $\sigma \in Isom_k(k(x), k(y))$ tel que $\sigma(x) = y$.
3) x et y ont même polynôme minimal sur k.

Démonstration. 1) ⇒ 3) Soient $\sigma \in Gal(\tilde{k} \setminus k)$ tel que $\sigma(x) = y$ et P le polynôme minimal de x sur k. On a :

$$P(y) = P(\sigma(x)) = \sigma(P(x)) = 0$$

Donc y est racine de P. Mais P est unitaire et irréductible sur $k[X]$. Donc P est nécessairement le polynôme minimal de y sur k.

3) ⇒ 2) Cela découle directement du lemme 12.

2) ⇒ 1) D'après le lemme précédent il existe $\tau \in Gal(\tilde{k} \setminus k)$ prolongeant σ. Ainsi $\tau(x) = y$, et x et y sont donc conjugués sur k.

□

Corollaire 30. Soit $x \in \tilde{k}$ de degré n.
- Il existe au plus n conjugués de x sur k, et ces conjugués sont les racines dans $\tilde{k}$ du polynôme minimal P de x sur k.
- Dire que x est séparable sur k signifie qu'il a n conjugués sur k.

Démonstration. Le point 1) est immédiat d'après le théorème précédent. Le point 2) découle du théorème précédent et de la proposition 19. □

Proposition 31. *Soit K une extension de k contenue dans $\tilde{k}$.*
- *Dire que K est normale sur k signifie que l'on a $\sigma(K) = K$ pour tout $\sigma \in Gal(\tilde{k} \setminus k)$.*

— *Supposons K normale sur k, et soit L une sous-extension de K. Pour tout $\sigma \in Hom_k(L, \tilde{k})$, on a $\sigma(L) \subset K$, et il existe $\tau in Gal(K \setminus k)$ induisant σ sur L.*

Démonstration. Premier point. Si l'extension $k \subset K$ est normale, K est alors un corps de décomposition de la famille des polynômes minimaux sur k des éléments de K. On les note $(P_i)_{i\in I}$. On note également $R_i \subset K$ l'ensemble des racines de P_i et R la réunion des R_i. On a $K = k(R)$. Si $\sigma \in Gal(\tilde{k} \setminus k)$, on a $\sigma(R_i) \subset R_i$ pour tout i et donc $\sigma(R) \subset R$. Il vient donc $\sigma(K) \subset K$ et en appliquant le lemme 27 $\sigma(K) = K$.

Second point. Il existe $\tau \in Gal(\tilde{k} \setminus k)$ prolongeant σ(lemme 27). K étant normale sur k, on a $\tau(K) = k$ d'après le point 1). D'où $\sigma(L) \subset K$, et τ induit un élément de $Gal(K \setminus k)$. □

Lemme 32. Soient $(K_i)_{i\in I}$ une famille non vide d'extensions normales de k contenues dans $\tilde{k}$ et

$$L = \bigcap_{i\in I} K_i, \text{ et } M = k\left(\bigcup_{i\in I} K_i\right)$$

Les extensions $k \subset L$ et $k \subset M$ sont normales.

Démonstration. Si $\sigma \in Gal(\tilde{k} \setminus k)$, il vient $\sigma(K_i) = K_i$ pour tout $i \in I$ d'après la proposition précédente. D'où $\sigma(L) = L$ et $\sigma(M) = M$. On conclut en utilisant à nouveau la proposition. □

Remarque 33. Compte tenue du lemme précédent, il existe une plus petite extension normale de k contenue dans $\tilde{k}$. On peut généraliser ce raisonnement.

Soit $\mathcal{E}$ une partie de $\tilde{k}$, et soit :

$$\mathcal{F} = \bigcup_{\sigma\in Gal(\tilde{k}\setminus k)} \sigma(\mathcal{E})$$

Si $\tau \in Gal(\tilde{k}\setminus k)$, on a $\tau(\mathcal{F}) = F$ et donc $\tau(k(\mathcal{F})) = k(\mathcal{F})$. Toujours d'après le même lemme l'extension $k(\mathcal{F})$ de k est normale. On dit que c'est l'extension normale de k engendrée par $\mathcal{E}$.

Proposition 34. Soit K une extension de k contenue dans $\tilde{k}$.

— Soit L l'extension normale engendrée par K. Si $[K : k]$ est fini, il en est de même pour $[L : k]$.

— Supposons K normale sur k. Alors K est une réunion de sous-extensions normales et de degré fini sur k.

Démonstration. Pour le premier point. Il existe une partie finie $\mathcal{E}$ de $\tilde{k}$ telle que $K = k(\mathcal{E})$. Si $x \in \mathcal{E}$, les conjugués de x sur k sont en nombre fini(corolaire 30). Il en résulte que, si $\mathcal{F} \subset \tilde{k}$ est associé à $\mathcal{E}$ comme dans la remarque précédente, alors $\mathcal{F}$ est finie. Par suite, $L = k(\mathcal{F})$ est une extension finie de k.

Pour le second point. Pour $x \in K$, soit L_x l'extension normale de k engendrée par x. D'après le point précédent, $[L_x : k]$ est fini. D'où le résultat. □

Théorème 35. Soit K une extension algébrique de k.
— L'extension $k \subset K$ possède une clôture normale.
— Deux extensions normales de l'extension $k \subset K$ sont k-isomorphes.

Démonstration. D'après le théorème 13, on peut supposer $K \subset \tilde{k}$. Il est alors clair que l'extension normale de k engendrée par K est une clôture normale de l'extension $k \subset K$. La seconde assertion découle directement de ce même théorème. □

0.2.5 Extensions galoisiennes

Définition 36. Une extension $k \subset K$ est dite galoisienne si elle est normale et séparable.

Proposition 37. Soit K une extension finie de k. Les conditions suivantes sont équivalentes.
1) K est galoisienne.
2) Il existe $P \in k[X] \setminus k$ séparable sur k tel que K soit un corps de décomposition de P sur k.
3) Il existe $Q \in K[X]$ irréductible et séparable sur k tel que K soit un corps de décomposition de Q sur k.

Démonstration. L'implication de 3) vers 2) est claire. Supposons 1) vérifiée. D'après le théorème de l'élément primitif, il existe $x \in K$ tel que $K = k(x)$. Soit Q le polynôme minimal de x sur k. Alors Q est irréductible, séparable et scindé sur K. Ainsi Q vérifie les conditions 3). Supposons maintenant 2) vérifiée. K est normale. En effet si l'on note $x_1, ..., x_n$ les racines de P alors $K = k[x_1, ..., x_n]$ est clairement normale. De plus P étant séparable l'extension K est galoisienne. □

Lemme 38. Soit $P \in k[X] \setminus k$, et D son corps de décomposition. Enfin on note $x_1, ..., x_n$ ses racines et S l'ensemble de ses racines. On a alors :

- Pour tout $\sigma \in Gal(D \setminus k)$ et tout $x \in S$, on a $\sigma(x) \in S$.
- Tout $\sigma \in Gal(D \setminus k)$ induit une permutation θ_σ de S.
- L'application $\theta : Gal(D \setminus k) \to \mathfrak{S}_S$, $\sigma \mapsto \theta_\sigma$ est un homomorphisme injectif de groupe.

Démonstration. Soit $\sigma \in Gal(D \setminus k)$. Les coefficients de P étant invariants par σ, on a $\sigma(x) \in S$, pour $x \in S$. Comme σ est une bijection de D sur lui même et que S est fini, σ induit bien une permutation θ_σ de S. Il est immédiat que l'on obtient ainsi un homomorphisme de groupe entre $Gal(D \setminus k)$ et $\mathfrak{S}_S$. On a $D = k(x_1, ..., x_n)$ et $\sigma_k = id_k$. L'application $\sigma : D \to D$ est donc entièrement déterminé par θ_σ, ce qui prouve que cet homomorphisme est injectif. □

0.3 Transcendance de π et e

Le but de cette section sera de prouver la transcendance de π et de e.

Lemme 39. Soit P un polynôme réel de degré m. Pour $z \in \mathbb{C}$, on pose :

$$I(P,z) = ze^z \int_0^1 e^{tz} P(tz)dt = z \int_0^1 e^{(1-t)z} P(tz)dt$$

Alors,

$$|I(P,z)| \leq |z|e^{|z|}\sup\{|P(tz)|; t \in [0,1]\}$$
$$I(P,z) = e^z \sum_{j=0}^{m} P^{(j)}(0) - \sum_{j=0}^{m} P^{(j)}(z)$$

Démonstration. Pour la majoration, on applique simplement l'inégalité triangulaire en majorant en plus le polynôme par son sup.

Pour l'égalité on distingue deux cas. Si z est nul alors c'est trivialement vrai. Sinon, on montre le résultat par récurrence sur m, en supposant $z \neq 0$. L'initialisation est immédiate. Pour l'hérédité, il résulte d'une intégration par partie :

$$I(P,z) = ze^z \left[-\frac{1}{2}e^{-zt}P(zt)\right]_0^1 + ze^z \int_0^1 e^{-zt}P'(zt)dt$$

$$= e^z P(0) - P(z) + I(P', z)$$

Ce qui prouve le résultat par récurrence.

□

Lemme 40. Soit $P \in \mathbb{Z}[X]$. Pour tout entier $n \in \mathbb{N}$, il existe un polynôme $P_n \in \mathbb{Z}[X]$ et tel que $P^{(n)} = n!P_n$.

Démonstration. Si $n > \deg(P)$ c'est le cas puisque $P^{(n)} = 0$. On suppose donc que $n \leq m = \deg(P)$. On écrit P de la façon suivante :

$$P(X) = a_m X^m + a_{m-1} X^{m-1} + ... + a_0$$

On obtient alors l'égalité suivante :

$$P^{(n)}(X) = n! \left(a_m \binom{m}{m-n} X^{m-n} + a_{m-1} \binom{m-1}{m-n-1} X^{m-n-1} + a_n \binom{n}{0} \right)$$

D'où le résultat. □

Remarque 41. Soit $P \in \mathbb{C}[X] \backslash \mathbb{C}$ de degré n. Il existe (Théorème de D'Alembert) $\lambda, \alpha_1, ..., \alpha_n$ tels que :

$$P(X) = \lambda \prod_{j=1}^{n} (X - \alpha_j)$$

Si f est une application de $\mathbb{C}$ dans lui même on pose :

$$\sum_{P(\alpha)=0} f(\alpha) = \sum_{j=1}^{n} f(\alpha_j)$$

Lemme 42. Soit $P \in \mathbb{Z}[X] \setminus \mathbb{Z}$ de coefficient dominant λ. Pour tout $n \in \mathbb{N}$ on a :

$$\lambda^n \sum_{P(\alpha)=0} \alpha^n \in \mathbb{Z}$$

Démonstration. On pose $Q = \lambda^{-1}P \in \mathbb{Q}[X]$.

Le polynôme Q est donc unitaire. Notons A sa matrice compagnon. On a donc $\lambda A \in M_m(\mathbb{Z})$, avec $m = \deg(P)$. Ceci implique que $\lambda^n A^n \in M_m(\mathbb{Z})$, et cela pour tout n entier. On a donc $tr(\lambda^n A^n) \in \mathbb{Z}$.

Si l'on note $\alpha_1, ..., \alpha_m$ les racines de P dans $\mathbb{C}$, les valeurs propres de λA sont $\lambda\alpha_1, ..., \lambda\alpha_m$. De même les valeurs propres de $\lambda^n A^n$ sont $\lambda^n\alpha_1^n, ..., \lambda^n\alpha_m^n$. La trace étant invariante par changement de base, en se plaçant dans une base de Jordan on obtient le lemme.

□

Lemme 43. Soit $P \in \mathbb{Z}[X] \setminus \mathbb{Z}$ tel que $P(0) \neq 0$. Alors

$$A = \sum_{P(\alpha)=0} e^{\alpha} \in \mathbb{C} \setminus \mathbb{Z}^*.$$

Démonstration. Posons r le degré de P et λ son coefficient dominant. Raisonnons par l'absurde et supposons que $A \in \mathbb{Z}^*$.

Soient p un entier premier et $Q(X) = X^{p-1}P^p(X)$. Le degré de Q est donc $p(1+r)-1$. Posons maintenant :

$$J_p = \sum_{P(\alpha)=0} I(Q, \alpha).$$

Ici $I(Q, \alpha)$ est défini comme dans le lemme 39. Soit D un disque fermé de $\mathbb{C}$, de centre 0 et de rayon R, contenant toutes les racines de P. Si $P(\alpha) = 0$, par le lemme 39 il résulte la majoration suivante :

$$|I(Q, \alpha)| \leq Re^R R^{p-1}(sup\{|P(z)|; z \in D\})^p.$$

Il existe donc un réel B indépendant de p et tel que :

$$|J_p| \leq B^p.$$

D'autre part, d'après le lemme 39 on a également :

$$J_p = \sum_{P(\alpha)=0} I(Q, \alpha)$$

$$= \sum_{P(\alpha)=0} \left(e^{\alpha} \sum_{n\geq 0} Q^{(n)}(0) - \sum_{n\geq 0} Q^{(n)}(\alpha) \right)$$
$$= A \left(\sum_{n\geq 0} Q^{(n)}(0) \right) - \sum_{n\geq 0} \left(\sum_{P(\alpha)=0} Q^{(n)}(\alpha) \right).$$

Si $P(\alpha) = 0$, alors α est un zéro d'ordre au moins p de Q, ce qui donne $Q^{(n)}(\alpha) = 0$ si $n < p$,(on applique directement la formule de Leibniz).

Si $n \geq p$, en appliquant le lemme 40, on peut poser $Q_n = (p!)^{-1} Q^{(n)} \in \mathbb{Z}[X]$. Maintenant, grâce au lemme 42, il vient :

$$\lambda^{m-n} \sum_{P(\alpha)=0} Q^{(n)}(\alpha) \in p!\mathbb{Z}.$$

Par ailleurs, on a $Q^{(n)}(0) = 0 \in p!\mathbb{Z}$ si $n < p-1$, et $Q^{(n)}(0) \in p!\mathbb{Z}$ si $n \geq p$, toujours d'après le lemme 40. Enfin, $Q^{(p-1)} = (p-1)!(P(0))^p$.

On déduit des remarques précédentes qu'il existe $M \in \mathbb{Z}$ tel que :

$$\frac{\lambda^{m-p}}{(p-1)!} J_p = \lambda^{m-p} A (P(0))^p + pM.$$

Par définition $m \geq p$, le second membre de l'égalité ci-dessus est donc un entier. De plus en utilisant le lemme de Gauss, si p ne divise pas $\lambda A P(0)$, alors il n'est pas un multiple de p. Quitte à prendre p suffisamment grand, c'est toujours le cas. En particulier, il est non nul, et donc supérieur ou égal à 1 en valeur absolue. Pour un tel p on peut écrire :

$$|J_p| \geq (p-1)!|\lambda|^{p-m} = (p-1)!|\lambda|^{1-pr}$$

Mais on a prouvé que $|J_p| \leq B^p$. Ainsi, pour p suffisamment grand :

$$(|\lambda|^r B)^p \geq |\lambda|(p-1)!$$

Ce qui est absurde, et conclut la preuve du lemme.

□

Les lemmes précédents, et en particulier le dernier sont des lemmes techniques qui seront au centre des preuves de transcendance de π et e.

0.3.1 Théorème d'Hermite

Théorème 44 (Théorème d'Hermite)**.** Le nombre réel e est transcendant sur le corps $\mathbb{Q}$.

Démonstration. Raisonnons par l'absurde, et supposons que ce n'est pas le cas. Alors il existe des entiers $a_0, ..., a_n$ non tous nuls, tels que $a_0 + a_1 e + ... + a_n e^n = 0$. Quitte à diviser par une puissance positive de e on peut supposer que $a_0 \neq 0$.

Soit p un nombre premier, et soit $P(X) = X^{p-1}(X-1)^p...(X-n)^p \in \mathbb{Z}[X]$. Avec les notations du lemme 39, posons :

$$J_p = a_0 I(P, 0) + ... + a_n I(P, n).$$

De la même façon que dans le lemme 43 il existe un réel B indépendant de p et tel que :

$$|J_p| \leq B^p.$$

En appliquant le lemme 39, on peut substituer $I(P, i)$ par son expression pour tout i, ce qui donne :

$$J_p = -\sum_{i=0}^{n} a_i \left(\sum_{j=0}^{np+p-1} P^{(j)}(i) \right) \in \mathbb{Z}.$$

Si $1 \leq i \leq n$, alors i est racine d'ordre p de P, et donc $P^{(j)}(i) = 0$ si $j < p$. On a aussi $P^{(j)}(i) \in p!\mathbb{Z}$ si $j \leq p$.

Par ailleurs, $P^{(j)}(0) = 0$ si $j < p-1$ et $P^{(j)}(0) \in p!\mathbb{Z}$ si $j \geq p$. Enfin, on a :

$P^{(p-1)}(0) = (p-1)!(-1)^p...(-n)^p = (-1)^{np}(p-1)!(n!)^p$.

On en déduit qu'il existe $N \in \mathbb{Z}$ tel que :

$$J_p = (-1)^{np+1} a_0 (p-1)!(n!)^p + p!N.$$

Prenons pour p un nombre premier vérifiant $p > n$ et ne divisant pas a_0. On a alors que $\dfrac{J_p}{(p-1)!}$ est un entier non divisible par p, et en particulier non

nul. Ce qui implique $|J_p| \geq (p-1)!$, et donc $B^p \geq (p-1)!$. On obtient alors une contradiction, ce qui conclut la preuve.

□

0.3.2 Théorème de Lindemann

Théorème 45 (Théorème de Lindemann)**.** Le nombre réel π est transcendant sur le corps $\mathbb{Q}$.

Démonstration. Raisonnons par l'absurde et supposons que π est algébrique sur $\mathbb{Q}$. Alors $i\pi$ l'est aussi. Notons P le polynôme minimal de $i\pi$ sur $\mathbb{Q}$. Les racines de P sont simples par la proposition 16 et le lemme 18. Notons les $\alpha_1, ..., \alpha_n$. Le corps $K = \mathbb{Q}(\alpha_1, ..., \alpha n)$ est le corps de décomposition de P dans $\mathbb{C}$, et l'extension $\mathbb{Q} \subset K$ est galoisienne par la proposition 37.

On rappelle que l'identité d'Euler est $e^{i\pi} + 1 = 0$. Il en résulte que $(1 + e^{\alpha_1})...(1 + e^{\alpha_n}) = 0$. On peut maintenant développer l'expression précédente, pour obtenir :

$$\sum_{\epsilon_1,...,\epsilon_n \in \{0,1\}} exp\left(\sum_{j=1}^{n} \epsilon_j \alpha_j\right) = 0$$

Posons :

$$R(X) = \prod_{\epsilon_1,...,\epsilon_n \in \{0,1\}} \left(X \sum_{j=1}^{n} \epsilon_j \alpha_j\right) \in K[X]$$

D'après le lemme 38, le groupe de Galois $Gal(K \setminus \mathbb{Q})$ opère sur l'ensemble des sommes de la forme $\epsilon_1\alpha_1 + ... + \epsilon_n\alpha_n$, avec $\epsilon_1, ..., \epsilon_n \in \{0, 1\}$. Pour $\sigma \in Gal(K \setminus \mathbb{Q})$, on note $\bar{\sigma}$ l'extension de σ à $K[X]$, on a $\bar{\sigma}(R) = R$. Or l'extension $\mathbb{Q} \subset K$ étant galoisienne, $R \in \mathbb{Q}[X]$. Par conséquent il existe $m \in \mathbb{N}^*$ tel que $mR \in \mathbb{Z}[X]$.

Soit $q \in \mathbb{N}^*$ l'ordre de la racine 0 du polynôme$R$, et soit $S \in \mathbb{Z}[X]$ tel que $R(X) = X^q S(X)$. On a $S(0) \neq 0$ et

$$\sum_{\epsilon_1,...,\epsilon_n \in \{0,1\}} exp\left(\sum_{j=1}^{n} \epsilon_j \alpha_j\right) = q + \sum_{S(\alpha)=0} e^{\alpha} = 0$$

Or ceci est impossible en vertu du lemme 43, on a donc une contradiction, et π est transcendant sur $\mathbb{Q}$.

□

Ces théorèmes ont été historiquement des révolutions. En effet, jusqu'aux travaux d'Hermite et Lindemann, les seuls nombres transcendants connus étaient artificiels et avaient été inventés dans ce but. La transcendance de π a également permis, (couplée aux travaux antérieurs de Wantzel sur les nombres constructibles) de répondre à l'un des plus vieux problèmes de mathématiques de l'époque : la quadrature du cercle.

0.4 Théorème de Liouville

Le but de cette section sera de prouver un théorème dû à Joseph Liouville et qui permet de caractériser les fonctions qui admettent des primitives "élémentaires" (dans un sens que l'on précisera ensuite). On montrera en particulier le résultat classique que e^{X^2} n'admet pas de primitives élémentaires.

0.4.1 Anneaux et corps différentiels

Définition 46. Soit B un anneau commutatif et A un sous anneau de B. Une dérivation de A dans B est une application $D : A \to B$ vérifiant pour tout $x, y \in A$, :

$$D(x+y) = D(x) + D(y)$$
$$D(xy) = xD(y) + yD(x)$$

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

Définition 47. Soit $n \in \mathbb{N}^*$, $A[\mathbf{X}] = A[X_1, ..., X_n]$, $P \in A[\mathbf{X}]$, et $D \in Der(A, B)$, on note P^D l'élément de $B[\mathbf{X}]$ définit par :

$$P^D(\mathbf{X}) = \sum_{\nu} D(a_\nu) X^\nu.$$

Définition 48. On appelle anneau différentiel un couple (A, D), où A est un anneau et D un élément de $Der(A, A)$. Dans ce cas, l'ensemble des $x \in A$ tel que $D(x) = 0$ est appelé l'anneau des constantes de (A, D).

Définition 49. Un corps différentiel est un couple (k, D) où k est un corps et D un élément de $Der(k, k)$. Dans ce cas, l'ensemble des $x \in k$ tel que $D(x) = 0$ est appelé le corps des constantes de (k, D).

Proposition 50. Soit K un corps, et A un sous-anneau de K. On note k le corps de fraction de A. Tout élément de $Der(A, K)$ se prolonge de manière unique en un élément de $Der(k, K)$.

Démonstration. Supposons que $D \in Der(A, K)$ se prolonge en un élément $\Delta \in Der(k, K)$. Alors pour $a \in A$ et $b \in A^*$ tel que $x \in k$ et $x = a/b$. Par les règles de dérivations on a nécessairement :

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

Pour obtenir le résultat, il suffit de vérifier que le résultat ne dépend pas de la représentation de x, et qu'elle définit bien une dérivation dans $Der(k, K)$.

Soit $c \in A^*$, il vient :

$$\frac{(bc)D(ac) - (ac)D(bc)}{(bc)^2} = \frac{bc^2D(a) + abcD(c) - ac^2D(b) - abcD(c)}{b^2c^2}$$

$$= \frac{bD(a) - aD(b)}{b^2}$$

Ce qui nous donne le premier point.

Soient $x = a/b$, $y = c/d$. Alors :

$$\Delta(x + y) = \Delta\left(\frac{ad + bc}{bd}\right) = \frac{bdD(ad + bc) - (ad + bc)D(bd)}{b^2d^2}$$

$$= \frac{bdD(ad) - adD(bd)}{b^2d^2} + \frac{bdD(bc) - bcD(bd)}{b^2d^2}$$

$$\Delta\left(\frac{ad}{bd}\right) + \Delta\left(\frac{bc}{bd}\right) = \Delta\left(\frac{a}{b}\right) + \Delta\left(\frac{c}{d}\right) = \Delta(x) + \Delta(y)$$

De même :

$$\Delta(xy) = \Delta\left(\frac{ac}{bd}\right) = \frac{bdD(ac) - (ac)D(bd)}{b^2d^2}$$

$$= \frac{bcdD(a) - acdD(b)}{b^2d^2} + \frac{abdD(c) - abcD(d)}{b^2d^2}$$

Que l'on peut réécrire :

$$\frac{cd}{d^2} \times \frac{bD(a) - aD(b)}{b^2} + \frac{ab}{b^2} \times \frac{dD(c) - cD(d)}{d^2}$$

$$= \frac{c}{d}\Delta\left(\frac{a}{b}\right) + = \frac{a}{b}\Delta\left(\frac{c}{d}\right) = y\Delta(x) + x\Delta(y)$$

Ce qui conclut le résultat.

□

Dans les deux résultats suivants, on posera $K = k(x_1, ..., x_n)$ une extension de type fini de k, et $\mathbf{x} = (x_1, .., x_n)$. On note $I_{\mathbf{x}} = \{P \in k[\mathbf{x}]; P(\mathbf{x}) = 0\}$.

Lemme 51. Soient $P, Q \in k[\mathbf{X}]$, $\mathbf{u} = (u_1, ..., u_n) \in K^n$, et $D \in Der(k, k)$. On suppose que $P \in I_{\mathbf{x}}$ et que :

$$P^D(\mathbf{x}) + \sum_{i=1}^{n} u_i \frac{\partial P}{\partial X_i}(\mathbf{u}) = 0$$

Alors,

$$(PQ)^D(\mathbf{x}) + \sum_{i=1}^{n} u_i \frac{\partial (PQ)}{\partial X_i}(\mathbf{u}) = 0$$

Démonstration. Un calcul direct montre que :

$$(PQ)^D(\mathbf{x}) = P^D(\mathbf{x})Q(\mathbf{x}) + Q^D(\mathbf{x})P(\mathbf{x})$$

et

$$\sum_{i=1}^{n} u_i \frac{\partial (PQ)}{\partial X_i}(\mathbf{u}) = P(\mathbf{x}) \sum_{i=1}^{n} u_i \frac{\partial Q}{\partial X_i}(\mathbf{u}) + Q(\mathbf{x}) \sum_{i=1}^{n} u_i \frac{\partial P}{\partial X_i}(\mathbf{u})$$

D'où le résultat en sommant les deux égalités. □

Remarque 52. On s'intéresse au problème de savoir si l'on peut prolonger la dérivée définit sur un corps dans l'une de ses extensions. Supposons que ce soit possible et notons Δ ce prolongement. Dans ce cas si $P \in I_{\mathbf{x}}$, on a alors $\Delta(P(\mathbf{x})) = 0$. On peut alors écrire :

$$P^D(\mathbf{x}) + \sum_{i=1}^{n} \Delta(x_i) \frac{\partial P}{\partial X_i}(\mathbf{x}) = 0$$

Or, d'après le lemme précédent, si cette relation est vérifié pour un système de générateurs de l'idéal $I_{\mathbf{x}}$ de $k[\mathbf{x}]$, elle l'est pour tout élément de $I_{\mathbf{x}}$.

Théorème 53. Soient $\mathbf{u} = (u_1, ..., u_n) \in K^n$, $D \in Der(k, k)$, et $(P_i)_{i \in I}$ un système de générateur de l'idéal $I_{\mathbf{x}}$ de $k[\mathbf{X}]$. Les conditions suivantes sont équivalentes :

— Il existe $\Delta \in Der(K, K)$ vérifiant $\Delta(x_j) = u_j$ pour tout $1 \leq j \leq n$ et prolongeant D.

— Pour tout $i \in I$, on a :

$$P_i^D(\mathbf{x}) + \sum_{j=1}^{n} u_j \frac{\partial P_i}{\partial X_j}(\mathbf{x}) = 0$$

De plus ces condition détermine Δ de manière unique.

Démonstration. L'implication découle immédiatement de la remarque précédente. Pour la réciproque, prenons $P \in k[\mathbf{X}]$ et posons :

$$\lambda(P) = P^D(\mathbf{x}) + \sum_{j=1}^{n} u_j \frac{\partial P}{\partial X_j}(\mathbf{x})$$

Un calcul direct montre que $\lambda(PQ) = P(\mathbf{x})\lambda(Q) + Q(\mathbf{x})\lambda(P)$

D'après le lemme 51, on a $\lambda(P) = 0$ pour tout $P \in I_{\mathbf{x}}$. Par suite si $P, Q \in k[\mathbf{X}]$ satisfont $P - Q \in I_{\mathbf{x}}$, alors $\lambda(P) = \lambda(Q)$. Il en résulte qu'il existe une application $\delta : k[x_1, ..., x_n] \to K$ et telle que $\delta(y) = \lambda(P)$, où $P \in k[\mathbf{X}]$ vérifie $y = P(\mathbf{x})$. On vient donc de montrer que $\delta \in Der(k[x_1, ..., x_n], K)$. Par ailleurs, il est clair que $\delta|k = D$. On peut donc prolonger δ en un élément $\Delta \in Der(K, K)$ par la proposition 50. L'unicité est claire par les conditions précédentes. □

Remarque 54. Supposons que $K = k(x)$ soit une extension simple de k. Notons I_x pour $I_{\{x\}}$. Soient $D \in Der(k, k)$ et $u \in K$. Distinguons plusieurs cas.

1) Si x est transcendant sur k. Alors $I_x = \{0\}$, et il existe donc une unique dérivation $\Delta \in Der(K, K)$ qui prolonge D et qui vérifie $\Delta(x) = u$.
2) Si x est algébrique et séparable sur k. Alors en notant P son polynôme minimal, la condition d'existence de Δ devient :

   $$P^D(x) + uP'(x) = 0$$

   Or x étant séparable, on a $P'(x) \neq 0$. Et donc Δ existe si et seulement si $u = -P^D(x)/P'(x)$.
3) Si x est algébrique et non séparable sur k. On a alors $\mathrm{car}(k) = p > 0$, et l'on a $P'(x) = 0$. La condition d'existence de Δ est donc $P^D(x) = 0$.

Proposition 55. Soient (k, D) un corps différentiel et K une extension algébrique séparable de degré fini de k. Il existe une et une seule dérivation $\Delta \in Der(K, K)$ telle que (K, Δ) soit une extension différentielle de (k, D).

Démonstration. D'après le théorème de l'élément primitif, il existe $x \in K$ tel que $K = k(x)$. Le résultat en découle, du fait que l'on est dans le cas 2 de la remarque précédente. □

Corollaire 56. Soit (k, D) un corps différentiel, et soit (K, Δ) une extension différentielle de (k, D). On suppose que K est une extension algébrique séparable de degré fini de k. Si $\sigma \in Gal(K \setminus k)$, on a $\Delta \circ \sigma = \sigma \circ \Delta$.

Démonstration. Soit $x \in K$, et $P \in k[X]$ son polynôme minimal sur k. D'après la proposition précédente :

$$\Delta(x) = \frac{-P^D(x)}{P'(x)}.$$

Comme $P \in k[X]$, on peut écrire :

$$\sigma \circ \Delta(x) = \frac{-P^D(\sigma(x))}{P'(\sigma(x))}.$$

Or, $\sigma(x)$ est une racine de P, et le polynôme minimal de $\sigma(x)$ sur k est donc P. En appliquant le début de la preuve à $\sigma(x)$ au lieu de x on obtient :

$$\Delta(\sigma(x)) = \frac{-P^D(\sigma(x))}{P'(\sigma(x))}.$$

D'où le résultat. □

0.4.2 Extensions élémentaires

Dans la suite, on considère des corps de caractéristique nulle. On désigne par (k, D) un corps différentiel, et on note k_0 son corps des constantes. Afin de simplifier la notation, si (K, Δ) est une extension différentielle de (k, D), on identifie k à un sous-corps de K et on note encore D pour Δ. Enfin si $a \in k$ on notera souvent a' pour $D(a)$.

Définition 57. 1) On dit que $t \in k$ est un logarithme de $a \in k^*$ si l'on a $t' = \frac{a'}{a}$.

2)On dit que $t \in k$ est une exponentielle de $a \in k$ si $\frac{t'}{t} = a'$.

Définition 58. Une extension 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 des constantes.

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

Définition 59. On dit que $x \in k$ est une somme de Liouville s'il existe $u \in k$, $v_1, ..., v_n \in k^*$ et $c_1, ..., c_n \in k_0$ tels que :

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

0.4.3 Théorème de Liouville

Dans ce qui suit on considère (K, D) une extension différentielle élémentaire de (k, D), et $x \in k$. De plus, on suppose vérifiées les conditions suivantes :

1) Le corps des constantes de K est k_0.

2) Il existe $t \in K$ tel que $K = k(t)$.

3) x est une somme de Liouville dans K, et donc de la forme $A + B$ avec :

$$A = u' \text{ et } B = \sum_{i=1}^{n} c_i \frac{v_i'}{v_i}$$

avec $u \in K$, $v_1, ..., v_n \in K^*$, et $c_1, ..., c_n \in k_0$.

Les deux lemmes suivants sont en fait la preuve du théorème de Liouville dans chacun des cas possibles d'extensions différentielles élémentaires, une fois ceux-ci prouvés le théorème en découlera immédiatement. Ils sont donc fondamentaux.

Lemme 60. Si t est algébrique sur k, alors x est une somme de Liouville dans k.

Démonstration. Soit L une clôture normale de l'extension $k \subset K$, elle existe toujours par le théorème 35. D'après le lemme 34, le corps L est de degré fini sur k, et comme car(k)= 0 par hypothèse, l'extension $k \subset L$ est galoisienne.

Par la proposition 55, il existe une unique dérivation Δ de L telle que (L, Δ) soit une extension différentielle de (k, D).

Posons $G = Gal(L \setminus k)$ et $m = [L : k]$. D'après le corolaire 56 on peut écrire :

$$\begin{aligned} mx &= \sum_{\sigma \in G} \sigma(x) = \sum_{\sigma \in G} \sigma(u') + \sum_{i=1}^{n} c_i \sum_{\sigma \in G} \frac{\sigma(v_i')}{v_i} \\ &= \left(\sum_{\sigma \in G} \sigma(u) \right)' + \sum_{i=1}^{n} c_i \sum_{\sigma \in G} \frac{\sigma(v_i)'}{v_i} \end{aligned}$$

Posons :

$$y = \frac{1}{m} \sum_{\sigma \in G} \sigma(u), \ zi = \frac{1}{m} \prod_{\sigma \in G} \sigma(v_i)$$

Ces éléments sont invariants par G, et donc appartiennent à k. Or on a :

$$x = y' + \sum_{i=1}^{n} c_i \frac{z_i'}{z_i}$$

Ce qui conclut la preuve. □

Lemme 61. On suppose maintenant que t est transcendant sur k, et que t est l'exponentielle d'un élément de k ou le logarithme d'un élément de k^*. Alors x est une somme de Liouville dans k.

Démonstration. On peut toujours identifier K au corps $k(T)$ des fractions rationnelles en l'indéterminé T sur k. Soit v, l'un des v_i. On a $v = P(t) \setminus Q(t)$ avec $P, Q \in k[T]$. On obtient donc l'égalité suivante :

$$\frac{D(v)}{v} = \frac{D(P(t))}{P(t)} - \frac{D(Q(t))}{Q(t)}.$$

On peut donc supposer que v est de la forme $P(t)$, $P \in k[t]$. Écrivons v sous la forme $v = \lambda \pi_1^{n_1}(t) ... \pi_r^{n_r}(t)$, avec $\lambda \in k^*$ et $\pi_1, ..., \pi_r \in k[T]$, unitaire et irréductible, et enfin $n_1, ..., n_r \in \mathbb{N}^*$. On a donc :

$$\frac{D(v)}{v} = \frac{D(\lambda)}{\lambda} + \sum_{j=1}^{r} n_j \frac{D(\pi_j(t))}{\pi_j(t)}.$$

On en déduit donc que A est de la forme :

$$A = \sum_i c_i \frac{a_i'}{a_i} + \sum_j c_j \frac{D(\pi_j(t))}{\pi_j(t)}.$$

où les c_i et les c_j sont dans k_0, les a_i sont dans k^*, et les π_j sont comme indiqués précédemment ;

L'élément u s'écrit comme $u = F(t)$ avec $F \in k(T)$. On peut donc prendre sa décomposition en éléments simples, qui nous donne :

$$u = P(t) + \sum_j \frac{P_j(t)}{\pi_j^{n_j}(t)}.$$

avec les n_j des entiers strictement positifs, $P, P_j, \pi_j \in k[T]$, les π_j sont unitaires et irréductibles et P_j premier avec π_j, et deg $(P_j) <$ n_j deg(π_j) pour tout j. On en déduit donc que B s'écrit :

$$B = D(P(t)) + \sum_j \frac{D(P_j(t))\pi_j(t) - n_j P_j(t) D(\pi_j(t))}{\pi_j^{n_j+1}(t)}$$

Raisonnons maintenant par disjonction de cas.

1) Supposons que t soit un logarithme de $a \in k^*$. On a donc $D(t) = \alpha \in k$. En reprenant les notations précédentes on peut écrire :

$$D(\pi_j(t)) = \pi_j^D(t) + \alpha \pi_j'(t).$$

Le polynôme π_j étant unitaire, on a deg$(\pi_j^D + \alpha\pi_j') <deg(\pi_j)$.

On en déduit donc que $P_j(\pi_j^D + \alpha\pi_j')$ et π_j sont premiers entre eux et de plus on a l'inégalité suivante : deg$(P_j(\pi_j^D + \alpha\pi_j') < (n_j + 1)deg(\pi_j)$.

Par conséquent, si π_j intervient dans u, il intervient à une puissance $n_j+1 \geq 2$ au dénominateur de u'. Comme il n'intervient qu'à une puissance au plus 1 dans le dénominateur de A c'est absurde, car x appartient à k. On vient donc de montrer que $u = P(t)$.

En appliquant le même raisonnement on obtient $D(\pi_j(t)) = 0$ pour tout π_j intervenant dans A. Ceci implique que $\pi_j(t) \in k_0$ et donc que t est algébrique ce qui est encore absurde puisqu'on l'a supposé transcendant. On peut donc réécrire x de la façon suivante :

$$x = D(P(t)) + \sum_i c_i \frac{a_i'}{a_i}$$

On a $D(P(t)) = P^D(t) + \alpha P'(t)$. Si $Q(T) = P^D(T) + \alpha P'(T)$, alors $Q \in k$. On va montrer que cela implique que $P(T) = cT + b$, avec $c_i n k_0$ et $b \in k$.

Posons $P(T) = p_n T^n + p_{n-1} T^{n-1} + ... + p_0$. On obtient donc que $D(P(t)) = p_n' t^n + (p_{n-1}' + n p_n \alpha) t^{n-1} + ... + (p_0' + p_1 \alpha)$.

Puisque $x \in k$ et que t est transcendant sur k, on a $p_n' = 0$, et donc $p_n \in k_0$. Par ailleurs si $n \geq 2$, on a $p_{n-1}' + n p_n \alpha = 0$.

Par suite, $D(p_{n-1} + n p_n t) = 0$, soit $p_{n-1} + n p_n t \in k_0$, ce qui est absurde puisque t est transcendant sur k. On a donc bien $P(T) = cT + b$. Enfin si on rassemble ce que l'on vient de montrer on obtient :

$$x = b' + c\frac{a'}{a} + \sum_i c_i \frac{a_i'}{a_i}$$

Ce qui démontre que x est bien une somme de Liouville dans k.

2) Supposons pour terminer que t soit une exponentielle de $a \in k$, soit $t' = a't$. Si $a' = 0$, alors $t \in k_0$ ce qui contredit le fait que t est transcendant sur k. On a donc $a' \neq 0$.

Soit π_j un facteur irréductible intervenant au dénominateur de B, et soit $Q_j(T) = \pi_j^D(T) + a'\pi_j'(T)T$. On obtient $\deg(Q_j) = \deg(\pi_j)$ et $D(\pi_j(t)) = Q_j(t)$.

Si Q_j n'est pas un multiple de π_j, alors π_j intervient au dénominateur de B avec une puissance $n_j + 1 \geq 2$. Comme au point précédent c'est absurde, et donc on peut écrire $u = P(t)$, et π_j n'intervient pas non plus dans l'expression de A.

Si maintenant Q_j est un multiple de π_j, on va montrer que dans ce cas $\pi_j(T) = T$. Posons :

$$\pi_j(T) = T^n + q_{n-1} T^{n-1} + ... + q_0$$

On a alors :

$$Q_j(T) = a' n T^n + (q_{n-1}' + a'(n-1) q_{n-1}) T^{n-1} + ... + (q_1' + a' q_1) T + q_0'$$

Si Q_j est multiple et si $q_l \neq 0$, on obtient $q_l' + a' l q_l = a' n q_l$, et donc :

$$\frac{q_l'}{q_l} = (n - l)\frac{t'}{t}$$

Ceci implique que $D(t^{n-l} \setminus q_l) = 0$,donc $t^{n-l} \in k$, ce qui est absurde puisque t est transcendant sur k. Donc $\pi_j(T) = T^n$ mais pi_j est irréductible d'où $\pi_j(T) = T$ Ce qui précède implique que :

$$u = \sum_j \alpha_j t^j$$

avec j positif ou négatif. On peut déduire que x est de la forme :

$$x = \sum_j (\alpha_j' + a' j \alpha_j) t^j + \sum_i c_i \frac{a_i'}{a_i} + c\frac{t'}{t}$$

$$= (\alpha_0' + a'c) + \sum_{j \neq 0} (\alpha_j' + a' j \alpha_j) t^j + \sum_i c_i \frac{a_i'}{a_i}$$

où $c \in k_0$.

Comme $x \in k$, les coefficients de t^j pour $j \neq 0$ sont nuls, donc $D(\alpha_j t^j) = 0$, si $j \neq 0$. Ainsi $\alpha_j t^j \in k_0$. Si $\alpha_j \neq 0$, on obtient à nouveau que t est algébrique ce qui est une contradiction. Finalement :

$$x = (\alpha_0 + ac)' + \sum_i c_i \frac{a_i'}{a_i}$$

est bien une somme de Liouville dans k.

□

Théorème 62 (Théorème de Liouville)**.** Soit (k, D) un corps différentiel, et soit $x \in k$. On suppose qu'il existe une extension élémentaire (K, D) de (k, D) et $y \in K$ vérifiant $y' = x$. Alors x est une somme de Liouville dans k.

Démonstration. Si $x = y'$ alors x est une somme de Liouville dans K. En conséquence le résultat est immédiat en itérant les deux lemmes précédents.
□

0.4.4 Application

On va prouver dans cette section plusieurs lemmes qui nous aiderons à appliquer ensuite le théorème précédent.

Lemme 63. Soit (K, D) une extension différentielle de (k, D) ayant k_0 pour corps des constantes. On suppose que $K = k(t)$ avec t transcendant sur k et

une exponentielle d'un élément de k. Si $x \in k$ alors les conditions suivantes sont équivalentes :

1) Il existe $y \in k$ tel que $x = y' + y\dfrac{t'}{t}$.

2) xt est une somme de Liouville dans K.

Démonstration. 1)⇒ 2) : On a $xt = ty' + yt' = (yt)'$.

2)⇒ 1) : On est dans le cas 2) de la preuve du lemme précédent, en remplaçant x par xt. On modifie néanmoins légèrement la fin du raisonnement. En reprenant les mêmes notations on trouve :

$$xt = (\alpha_0' + a'c) + \sum_{j \neq 0} (\alpha_j' + a' j \alpha_j) t^j + \sum_i c_i \frac{a_i'}{a_i}$$

avec $t' = a't$. On doit maintenant considérer les termes de degrés 1 en t, ce qui donne :

$$x = \alpha_1' + a'\alpha_1 = \alpha_1' + \alpha_1 \frac{t'}{t}$$

On a donc le résultat. □

Lemme 64. Soit (K, D) une extension différentielle de (k, D) ayant k_0 pour corps des constantes, et $x \in k$.

1) Si $y \in K \setminus k$ vérifie $D(y) = x$ alors y est transcendant sur k.

2) Si $y \in K$ est une exponentielle de x, alors y est transcendant sur k si et seulement si nx n'est pas un logarithme d'un élément de k^* pour tout entier $n \in \mathbb{N}^*$.

Démonstration. 1) Supposons par l'absurde que y est algébrique sur k, et soit P son polynôme minimal sur k : $P(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$.

On a $n \geq 2$. Posons $Q(X) = P^D(X) + xP'(X)$, alors $D(P(y)) = Q(y) = 0$. Comme $\deg(Q) < n$, on obtient $Q = 0$ par contradiction de la minimalité de P. En particulier, $nx + a_{n-1}' = 0$, soit $ny + a_{n-1} \in k_0$ ce qui est absurde puisque $y \notin k$.

2) Supposons que $y' = x'y$ et que y soit algébrique sur k. Avec les mêmes notations que précédemment, soit $R(X) = P^D(X) + x'XP'(X)$. On obtient $D(P(y)) = R(y) = 0$.

Si $x' \neq 0$, alors $\deg(Q) = n$, donc P et R sont proportionnels, et $R = nx'$. En particulier, on a $a_0' = nx'a_0$, ce qui montre que nx est un logarithme de a_0.

Si $x' = 0$, alors x est un logarithme de 1.

Réciproquement, supposons qu'il existe $n \in \mathbb{N}^*$ et tel que nx soit un logarithme de $\alpha \in k^*$. On a alors que $D(y^n \setminus \alpha) = 0$ ce qui donne $y^n = c\alpha$, avec $c \in k_0$. Et donc y est algébrique sur k.

□

Dans la suite on étudie le cas où $k = \mathbb{C}(X)$, muni de la dérivation usuelle D. On considère également (K, D) une extension différentielle de (k, D), et $g \in k$. Par abus de notation, on note e^g tout élément de K qui est une exponentielle de g. Une primitive de g dans K est un élément G de K vérifiant $G' = g$.

Lemme 65. Soit (K, D) une extension différentielle de (k, D), et $g \in k$. On suppose également que le corps des constantes de (K, D) est $\mathbb{C}$. Alors les conditions suivantes sont équivalentes :

1) $g \notin \mathbb{C}$

2) e^g est transcendant sur k.

Démonstration. Pour toute exponentielle $h \in K$ de g, on a $D(h) = D(g)h$. Si $g \in \mathbb{C}$, il vient $D(h) = 0$, donc $h \in \mathbb{C}$ et h n'est pas transcendant.

Supposons donc que $g \notin \mathbb{C}$. Pour montrer que e^g est transcendant sur k, il suffit, d'après le lemme 24, de montrer que ng n'est pas un logarithme d'un élément de k^* pour tout $n \in \mathbb{N}^*$.

Notons $ng = R(X) \in \mathbb{C}(X)$, et supposons que $h = S(X) \in \mathbb{C}(X)$ vérifie la relation suivante :

$$\frac{S'(X)}{S(X)} = R'(X)$$

Écrivons $S(X) = P_1^{n_1}(X)...P_r^{n_r}(X)$, où les P_i sont des polynômes irréductibles, de $\mathbb{C}[X]$, deux à deux distincts, et où les n_i sont des éléments de $\mathbb{Z} \setminus \{0\}$, et $R = P \setminus Q$, où $P, Q \in \mathbb{C}[X]$, sont premiers entre eux. On a alors l'égalité suivante :

$$\sum_{i=1}^{r} n_i \frac{P_i'}{P_i} = \frac{P'Q - Q'P}{Q^2}$$

Comme $\deg(P_i') < \deg(P_i)$, le membre gauche de cette égalité est la décomposition en éléments simples du membre de droite. Il en résulte que les pôles du second membres sont simples, et donc que Q divise $P'Q - Q'P$.

Or les polynômes P et Q sont premiers entre eux, donc Q divise Q'. Ceci n'est possible que si Q est constant. On peut donc réécrire l'égalité précédente :

$$\sum_{i=1}^{r} n_i \frac{P_i'}{P_i} = \lambda P'$$

avec $\lambda \in \mathbb{C}$. La décomposition en élément simple étant unique, il vient $P' = 0$. Donc $g \in \mathbb{C}$ ce qui est absurde et conclut la preuve.

□

Proposition 66. La fonction e^{X^2} n'admet pas de primitive élémentaire.

Démonstration. Soient $f \in k \setminus \{0\}$, $g \in k \setminus \mathbb{C}$, et (K, D) une extension élémentaire de (k, D). Supposons qu'il existe un élément de K qui soit une exponentielle de g. Notons cet élément e^g.

D'après le lemme 25 cet élément est transcendant sur k. Par ailleurs, $k(e^g)$ est une extension élémentaire de k, et K une extension élémentaire de $k(e^g)$ et de k.

Supposons qu'il existe une primitive élémentaire de fe^g dans K. Dans ce cas fe^g est une somme de Liouville dans K. En appliquant le théorème de Liouville c'est une somme de Liouville dans $k(e^g)$. Compte tenu du lemme 23, il existe $y \in k$ tel que

$$f = y' + yg'.$$

Si l'on considère le cas $f = 1$ et $g = X^2$, on obtient :

$$1 = y' + 2Xy.$$

Distinguons les cas. Supposons $y \in \mathbb{C}(X) \setminus \mathbb{C}[X]$. Soit α un pôle de y d'ordre n. Alors α est un pôle de y' d'ordre $n + 1$, ce qui est absurde. On a donc $y \in \mathbb{C}[X]$.

Mais dans ce cas $\deg(y' + 2Xy) \geq 1$. Ce qui est une contradiction. On vient donc de prouver qu'il n'existe aucune extension élémentaire de $(\mathbb{C}(X), D)$ dans laquelle e^{X^2} ait une primitive.

□

Remarque 67. La définition de primitive élémentaire correspond bien à l'intuition. En effet en partant du corps $\mathbb{C}(X)$ les extensions élémentaires contiennent toutes fonctions que l'on peut former en un nombre fini d'opérations (celles du corps, et la composition) à partir des polynômes, des fractions rationnelles, des racines nièmes, des exponentielles, des logarithmes, des constantes ainsi que toutes les fonctions trigonométrique circulaires et hyperboliques ainsi que leurs réciproques grâces aux formules d'Euler.

On peut néanmoins décider de rajouter l'opération "prendre une primitive", on obtiendrait alors la classe des fonctions dites Liouvilliennes, dont cette fois ci e^{X^2} fait naturellement parti. On pourrait alors étendre le théorème de Liouville et montrer que certaines fonctions ne sont pas Liouviliennes (c'est par exemple le cas de certaines fonctions de Bessel). Enfin certaines fonctions (dites hyper-transcendantes) ne sont solution d'aucune équation différentielle algébrique à coefficients entiers. C'est par exemple le cas de la fonction Γ (théorème de Hölder). Pour développer cela il faudra s'intéresser à une théorie plus forte que celle développer ici : la théorie de Galois différentielle.

0.5 Conclusion

Dans ce mémoire, nous avons étudié des notions de théorie des corps, de théorie de Galois, qui ont permis de démontrer d'intéressants résultats d'impossibilité. Il est important de noter que c'est un des premiers exemples historiques de rapprochement de branches des mathématiques à priori distinctes et qui a conduit à résoudre des problèmes qui étaient non résolus depuis des centaines d'années. On peut également noter que les idées de Galois ont été massivement utilisées et généralisées au XX et XXI siècle notamment en géométrie algébrique ou plus récemment encore au sein du programme de Langlands.

Bibliographie

[1] Tauvel, Patrice. Corps commutatifs et théorie de Galois. éditions Calvage et Mounet, Série mathématique en devenir (2021). ISBN : 9782916352879. https://books.google.fr/books?id=rCqYzgEACAAJ.

[2] Liouville, Joseph. "Mémoire sur l'intégration d'une classe de fonctions transcendantes.." Journal für die reine und angewandte Mathematik 13 (1835) : 93-118. ISSN : 0075-4102 ; 1435-5345/e. http://eudml.org/doc/146925.

[3] Hermite, Charles "Sur la fonction exponentielle", Comptes rendus hebdomadaires des séances de l'Académie des sciences, vol. 77, 1873, p.18-24, 74-79, 226-233 et 285-293. http://www.bibnum.education.fr/mathematiques/theorie-des-nombres/la-demonstration-de-la-transcendance-de-e

[4] Lindemann, Ferdinand. "Ueber die Zahl π.)." Mathematische Annalen 20 (1882) : 213-225. https://www.semanticscholar.org/paper/Ueber-die-Zahl-%CF%80.*)-Lindemann/e128c9891c68e627d0480153d017dbabbd9cd4b7

[5] https://en.wikipedia.org/wiki/Elementary_function?oldid=591752844

[6] https://en.wikipedia.org/wiki/Liouville%27s_theorem_(differential_algebra)

[7] https://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_de_Krull