Les calculatrices, téléphones, tablettes, ordinateurs, montres connectées et tous appareils électroniques de communication ou de stockage, ainsi que les documents sont interdits.

La qualité de la rédaction est un facteur important d'appréciation des copies. Les candidats sont donc invités à produire des raisonnements clairs, complets et concis.

Les candidats peuvent utiliser les résultats énoncés dans les questions ou parties précédentes, en veillant dans ce cas à préciser la référence du résultat utilisé.

Définitions, notations et rappels

Si a et b sont deux entiers tels que $a \leqslant b$, on désigne par $[\![a, b]\!]$ l'ensemble des entiers compris au sens large entre a et b.

Tous les corps considérés sont commutatifs.

Soit K un corps.
On note 0 et 1 ses éléments neutres respectivement pour l'addition et la multiplication.
On note K^* l'ensemble des éléments non nuls de K.
Si (x, y) est un élément de $K \times K^*$, l'élément xy^{-1} peut aussi être noté $\frac{x}{y}$.

On désigne par $K[X]$ la K-algèbre des polynômes à coefficients dans K et par $K(X)$ le corps des fractions rationnelles à coefficients dans K. Si P est dans $K[X]$, on note P' son polynôme dérivé. Si R est dans $K(X)$, on note de même R' sa fraction dérivée. On rappelle que si P et Q sont des polynômes de $K[X]$, avec Q non nul, tels que $R = P/Q$, alors $R' = (P'Q - Q'P)/Q^2$.

Une partie non vide k du corps K, qui est un corps pour les lois d'addition et de multiplication induites par celles de K est appelée un *sous-corps* de K.
On dit que L/K est une *extension de corps* si L est un corps vérifiant $K \subseteq L$ et K est un sous-corps de L. On dit aussi dans ce cas que L est un *surcorps* de K.
Si L/K est une extension de corps, L est naturellement muni d'une structure de K-espace vectoriel. On dit que l'extension de corps L/K est *finie* si L est de dimension finie en tant que K-espace vectoriel. On note alors $\dim_K(L)$ la dimension du K-espace vectoriel L. On appelle K-base de L une base du K-espace vectoriel L.

On rappelle que si M/L et L/K sont deux extensions finies, alors M/K l'est également ; on pourra utiliser sans démonstration la *formule de multiplicativité des degrés*

$$\dim_K(M) = \dim_K(L)\dim_L(M).$$

Si L/K est une extension de corps, on désigne par $\mathrm{Aut}_K(L)$ l'ensemble des automorphismes de corps de L dont la restriction à K est l'identité. On admet que c'est un groupe pour la composition.

Soit L/K une extension de corps et soit x un élément de L.
On note $K[x]$ le plus petit sous-anneau de L (au sens de l'inclusion) contenant K et x, et $K(x)$ le plus petit sous-corps de L (au sens de l'inclusion) contenant K et x. On rappelle que

$$K[x] = \{P(x) \mid P \in K[X]\} \quad \text{et} \quad K(x) = \left\{ \frac{P(x)}{Q(x)} \mid (P, Q) \in K[X]^2,\ Q(x) \neq 0 \right\}.$$

On définit de plus l'*idéal annulateur* de x comme

$$\mathrm{Ann}_{x,K} = \{P \in K[X] \mid P(x) = 0\}.$$

On ne demande pas de justifier qu'il s'agit d'un idéal.
Lorsque l'idéal $\mathrm{Ann}_{x,K}$ est réduit à $\{0_{K[X]}\}$, on dit que x est *transcendant* sur K. Dans le cas contraire, c'est-à-dire lorsque l'idéal $\mathrm{Ann}_{x,K}$ contient au moins un polynôme non nul, on dit que x est *algébrique* sur K ; dans ce cas, l'idéal $\mathrm{Ann}_{x,K}$ est engendré par un unique polynôme unitaire de $K[X]$, appelé *polynôme minimal* de x sur K et noté $\mu_{x,K}$, ou simplement μ_x s'il n'y a pas d'ambiguïté sur le corps K. On rappelle que $\mu_{x,K}$ est un polynôme irréductible de $K[X]$.

Si p est un nombre premier, si k est un entier naturel non nul et $q = p^k$, on note $\mathbb{F}_q$ le corps à q éléments. Dans le cas particulier où $k = 1$, et donc $q = p$, on a simplement $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Dans tout le problème, les corps de caractéristique nulle sont des surcorps de $\mathbb{Q}$, et, pour tout nombre premier p, les corps de caractéristique p sont des surcorps de $\mathbb{F}_p$.

Exercice

1. Justifier que le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Q}$.

2. Justifier que $(1, \sqrt[3]{2}, \sqrt[3]{4})$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt[3]{2}]$.

On pose $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. On définit l'application

$$m_\alpha : \begin{array}{ccc} \mathbb{Q}[\sqrt[3]{2}] & \longrightarrow & \mathbb{Q}[\sqrt[3]{2}] \\ y & \longmapsto & \alpha y \end{array}$$

Il s'agit d'un endomorphisme du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt[3]{2}]$, ce qu'on ne demande pas de justifier.

3. Écrire la matrice de m_α sur la base $(1, \sqrt[3]{2}, \sqrt[3]{4})$.

4. Déterminer le polynôme caractéristique de m_α.

5. En déduire le polynôme minimal de m_α.

Problème

Partie I

Dans toute cette partie, on fixe une extension de corps L/K.

1. Soit x un élément de L.

(a) Justifier qu'il existe un morphisme de K-algèbres $\Phi : K[X] \to K[x]$ tel que $\Phi(X) = x$, dont la restriction à K est l'identité. Préciser son noyau.

(b) On suppose que x est transcendant sur K. Démontrer que $K[X]$ et $K[x]$ sont des K-algèbres isomorphes et en déduire que $K(X)$ et $K(x)$ le sont aussi. Justifier alors que $K(x)$ est de dimension infinie en tant que K-espace vectoriel.

(c) Soit x un élément de L algébrique sur K. Démontrer que $K(x) = K[x]$, puis que $K(x)$ est de dimension finie (en tant que K-espace vectoriel), de dimension égale à $\deg(\mu_x)$. Donner une K-base de $K(x)$.

Dans les questions **2** et **3**, x désigne un élément de L algébrique sur K.

2. Démontrer que si μ_x admet une racine au moins double, alors son polynôme dérivé μ'_x est le polynôme nul.

3. Déterminer l'ensemble des polynômes P de $K[X]$ dont le polynôme dérivé est nul selon que K est de caractéristique nulle ou de caractéristique $p > 0$.

En déduire que, si K est un corps de caractéristique nulle ou un corps fini, alors μ_x est à racines simples.

Indication : Dans le cas où K est un corps fini de caractéristique $p > 0$, on pourra raisonner par l'absurde et utiliser, en le justifiant, le fait que l'application $x \mapsto x^p$ est un morphisme de corps surjectif.

On note $\mathcal{L}_K(L)$ la K-algèbre des endomorphismes du K-espace vectoriel L.
Pour tout x dans L, on définit l'application de multiplication par x :

$$m_x : \begin{array}{ccc} L & \longrightarrow & L \\ y & \longmapsto & xy \end{array}.$$

Alors $m_x \in \mathcal{L}_K(L)$, ce qu'on ne demande pas de justifier.

4. Démontrer que l'application $x \mapsto m_x$ est un morphisme injectif de K-algèbres de L dans $\mathcal{L}_K(L)$. En déduire

$$\forall x \in L,\ \forall P \in K[X], \quad m_{P(x)} = P(m_x),$$

puis que, pour tout élément x de L algébrique sur K, le polynôme minimal de l'endomorphisme m_x existe et est égal à μ_x.

5. On suppose **uniquement dans cette question** que $L = K(x)$, où x est un élément de L algébrique sur K. On pose $d = \deg(\mu_x)$ et $\mu_x = X^d + \sum_{i=0}^{d-1} a_i X^i$, avec $a_0, \ldots, a_{d-1}$ dans K. Démontrer que, dans une base convenable, la matrice représentative de m_x est la matrice compagnon associée à μ_x, c'est-à-dire la matrice carrée d'ordre d

$$C = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d-2} \\ 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

Dans la suite de cette partie, on suppose que L/K est une extension finie. Pour tout x dans L, on pose

$$\mathrm{tr}_{L/K}(x) = \mathrm{tr}(m_x) \quad \text{et} \quad \mathrm{N}_{L/K}(x) = \det(m_x),$$

où $\mathrm{tr}(m_x)$ et $\det(m_x)$ désignent la trace et le déterminant de l'endomorphisme $m_x \in \mathcal{L}_K(L)$.

6. Justifier que, pour tout x dans L, $\mathrm{tr}_{L/K}(x)$ et $\mathrm{N}_{L/K}(x)$ sont dans K.

7. (a) Justifier que l'application $\mathrm{tr}_{L/K} : L \to K$ est K-linéaire, et que

$$\forall (x,y) \in L^2, \quad \mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y).$$

Vérifier que

$$\forall x \in L^*, \quad \mathrm{N}_{L/K}(x) \neq 0.$$

(b) Pour tout u dans K, calculer $\mathrm{tr}_{L/K}(u)$ et $\mathrm{N}_{L/K}(u)$.

Dans les trois questions suivantes, on fixe un élément x de L.

8. Justifier que x est algébrique sur K.

On note $d = \deg(\mu_x)$.

9. Soit $a = \dim_{K(x)}(L)$ et soit $(\ell_1, \ldots, \ell_a)$ une $K(x)$-base de L. Démontrer que $(\ell_i \cdot x^{j-1})_{\substack{1 \leqslant i \leqslant a \\ 1 \leqslant j \leqslant d}}$ est une K-base de L.

10. En ordonnant convenablement la base de la question **9**, construire une K-base de L dans laquelle la matrice représentative de m_x est diagonale par blocs, de la forme :

$$\begin{pmatrix} C & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & C \end{pmatrix},$$

où C est la matrice compagnon associée à μ_x, définie dans la question **5**.

On pose $n = \dim_K(L)$. Soit $x_1, \ldots, x_d$ les racines (comptées avec leurs multiplicités) de μ_x dans son corps de décomposition sur K. Justifier que

$$\mathrm{tr}_{L/K}(x) = \frac{n}{d}\sum_{i=1}^{d} x_i \quad \text{et} \quad \mathrm{N}_{L/K}(x) = \left(\prod_{i=1}^{d} x_i\right)^{\frac{n}{d}}.$$

Notations pour la suite du problème

Soit A un anneau commutatif unitaire. Une application $D : A \to A$ est une *dérivation* sur A si elle vérifie les deux propriétés suivantes :

$$\forall (u, v) \in A^2, \quad D(u+v) = D(u) + D(v) \quad \text{et} \quad D(u \cdot v) = u \cdot D(v) + D(u) \cdot v.$$

On admet que si D et D' sont deux dérivations sur A, alors pour tous a, b éléments de A, $aD + bD'$ est une dérivation.
On appelle *corps différentiel* un couple (K, D) où K est un corps et D une dérivation sur K. Lorsqu'il n'y a pas d'ambiguïté sur la dérivation, on parlera du corps différentiel K.
On note $\mathrm{Der}(K)$ l'ensemble des dérivations sur K et on admet que c'est un K-espace vectoriel.

Le corps des fractions rationnelles $K(T)$ est muni d'une dérivation dite « usuelle » $\partial : R \mapsto R'$ dont la restriction à $K[T]$ vérifie pour rappel

$$\forall d \in \mathbb{N}, \ \forall (a_i)_{0 \leqslant i \leqslant d} \in K^{d+1}, \quad \partial\left(\sum_{i=0}^{d} a_i X^i\right) = \left(\sum_{i=0}^{d} a_i X^i\right)' = \sum_{i=1}^{d} a_i i X^{i-1}.$$

Cette dérivation fait de $(K(T), \partial)$ un corps différentiel ; il n'est pas demandé de le démontrer.

Si (K, D) est un corps différentiel, alors l'ensemble

$$K_{\text{cst}} = \{x \in K \mid D(x) = 0\}$$

est appelé l'ensemble des *constantes* de K. Notons que la définition de K_{cst} dépend de D, mais on omet d'indiquer D pour alléger les notations.

Soit (K, D) un corps différentiel. Pour tout $P = \sum\limits_{i=0}^{n} a_i X^i$ dans $K[X]$, on définit un polynôme de $K[X]$, noté P^D, en posant

$$P^D = \sum_{i=0}^{n} D(a_i) X^i.$$

Si (L, D) est un corps différentiel et K un sous-corps de L, on dit que $(L/K, D)$ est une *extension différentielle* si la dérivation $D : L \to L$ vérifie

$$D(K) \subseteq K, \quad \text{et} \quad L_{\text{cst}} = K_{\text{cst}}.$$

On peut dire aussi que (L, D) est une extension différentielle de (K, D), ou plus simplement que L/K est une extension différentielle s'il n'y a pas d'ambiguïté.
On remarque et on admet que si (L, D) est une extension différentielle de K, alors $(K, D_{|K})$ est aussi un corps différentiel, où $D_{|K}$ désigne la restriction de D à K.
L'égalité ensembliste $L_{\text{cst}} = K_{\text{cst}}$ implique en particulier que si L est un surcorps différentiel de K, alors tout élément x de L vérifiant $D(x) = 0$ est dans K et donc, par contraposée, on a :

$$\forall x \in L \setminus K, \ D(x) \neq 0.$$

Partie II

Soit (K, D) un corps différentiel fixé pour l'intégralité de la partie II.

II.1 – Formulaire de calcul.

11. Justifier que $D(1) = 0$, et donner, pour tout élément x de K^*, une relation entre $D\left(\frac{1}{x}\right)$ et $D(x)$.

12. Soit $(x, y) \in K \times K^*$. Démontrer les identités suivantes :

$$\forall n \in \mathbb{N} \setminus \{0\},\ D(x^n) = nx^{n-1}D(x) \quad \text{et} \quad D\left(\frac{x}{y}\right) = \frac{D(x)y - xD(y)}{y^2}.$$

Démontrer que si x est non nul, alors la première relation vaut pour tout n dans $\mathbb{Z}$.

13. Vérifier que K_{cst} est un sous-corps de K et que D est une application K_{cst}-linéaire.

14. Soit L_D l'application définie par :

$$L_D : x \longmapsto \frac{D(x)}{x}.$$

(a) Démontrer que L_D est un morphisme de groupes de $(K^*, \times)$ dans $(K, +)$. Déterminer son noyau.

(b) Dans cette question, on considère le cas particulier $K = k(X)$ où k désigne un corps. Déduire de la question précédente que pour tout R dans $k(X)$, tel que R se factorise sous la forme $R = c\prod_{i=1}^{r}(X - \alpha_i)^{\beta_i}$, avec c dans k^*, les α_i dans k et les β_i dans $\mathbb{Z}$, on a :

$$\frac{D(R)}{R} = \frac{D(c)}{c} + \sum_{i=1}^{r} \beta_i \frac{D(X - \alpha_i)}{X - \alpha_i}.$$

II.2 – Construction et extension de dérivations.

Soit p un nombre premier, k un entier naturel non nul et $q = p^k$. On rappelle que $\mathbb{F}_q$ désigne le corps à q éléments.

15. Dans cette question, $p = 2$ et $q = 4$. Démontrer qu'il existe j dans $\mathbb{F}_4$ tel que $\mathbb{F}_4 = \mathbb{F}_2(j)$, et $j^2 + j + 1 = 0$.

Soit D une dérivation sur $\mathbb{F}_4$. Que vaut $D(j^3)$? En déduire l'ensemble des dérivations sur $\mathbb{F}_4$.

16. On revient au cas général. Déterminer l'ensemble des dérivations sur le corps fini $\mathbb{F}_q$.

On suppose dans tout le reste de la partie II.2 que K est un corps de caractéristique nulle.

17. Soit K' un corps isomorphe à K et soit $\Phi : K' \to K$ un isomorphisme de corps. Démontrer que l'application

$$D' = \Phi^{-1} \circ D \circ \Phi$$

définit une dérivation sur K', et que $K'_{\text{cst}} = \Phi^{-1}(K_{\text{cst}})$.

Soit L un surcorps de K et $\widehat{D}$ une dérivation sur L. On note $\widehat{D}_{|K}$ la restriction de $\widehat{D}$ à K. On dit que $\widehat{D}$ *prolonge* la dérivation D si $\widehat{D}_{|K} = D$.
L'objectif des questions suivantes est de démontrer que sous certaines hypothèses, on peut construire sur L une dérivation $\widehat{D}$ qui prolonge la dérivation D.

18. Soit A un anneau commutatif intègre et soit B son corps de fractions. On rappelle que $B = \{\frac{a}{b} \ ; \ (a,b) \in A \times A \setminus \{0\}\}$. Démontrer que toute dérivation D sur A se prolonge de manière unique en une dérivation sur B.

Pour les questions **19** à **21**, on rappelle que la notation P^D a été introduite à la page de notations qui précède la partie II.

19. On suppose dans cette question que $L = K(x)$, où x est un élément de L transcendant sur K.
Construire une dérivation $\widehat{D}$ sur L dont la restriction à $K[x]$ est l'application qui, pour tout polynôme P dans $K[X]$, envoie $P(x)$ sur $P^D(x)$. Vérifier alors que la dérivation $\widehat{D}$ ainsi construite prolonge D.

On suppose, dans les questions **20** à **22**, que $L = K(x)$, où x est un élément de L **algébrique** sur K.

20. Démontrer l'existence de Q dans $K[X]$ tel que

$$\mu_x^D(x) + Q(x)\mu_x'(x) = 0.$$

21. Soit Q un polynôme vérifiant l'égalité de la question précédente. Démontrer que l'image de l'idéal $\mu_x K[X]$ par l'application :

$$\begin{array}{rcl} K[X] & \longrightarrow & K[X] \\ P & \longmapsto & P^D + Q \cdot P' \end{array}$$

est incluse dans $\mu_x K[X]$. En déduire que cette application induit une dérivation sur L dont la restriction à K est D.

22. Démontrer que si $(K(x), D_1)$ et $(K(x), D_2)$ sont deux corps différentiels tels que $D_{1|K} = D_{2|K} = D$, alors $D_1 = D_2$.

23. On suppose que L/K est une extension finie. Justifier qu'il existe un unique prolongement de D en une dérivation sur L. On rédigera précisément une démonstration par récurrence sur $\dim_K(L)$.

24. Soit L/K une extension finie et D une dérivation sur $K(X)$. Justifier brièvement que $L(X)$ est une extension finie de $K(X)$ et qu'il existe une unique dérivation sur $L(X)$ qui prolonge D.

25. On suppose dans cette question uniquement que K est de dimension finie sur $\mathbb{Q}$. Déterminer l'ensemble des dérivations sur K.

26. Soit $(L/K, D)$ une extension différentielle finie. Démontrer

$$\forall \sigma \in \mathrm{Aut}_K(L), \ \sigma \circ D = D \circ \sigma.$$

Il reste à étudier si ce résultat d'existence et d'unicité se prolonge aux corps infinis de caractéristique non nulle.
Soit p un nombre premier, k un entier naturel non nul et $q = p^k$.
On note $0_{\mathrm{Der}} : \mathbb{F}_q(X^q) \to \mathbb{F}_q(X^q)$ l'application nulle et on rappelle que $\mathrm{Der}(\mathbb{F}_q(X))$ désigne le $\mathbb{F}_q(X)$-espace vectoriel des dérivations sur $\mathbb{F}_q(X)$.

27. Démontrer que $\mathbb{F}_q(X)/\mathbb{F}_q(X^q)$ est une extension finie et qu'il n'y a pourtant pas unicité du prolongement de 0_{Der} en une dérivation de $\mathbb{F}_q(X)$.

28. Démontrer que l'application :

$$\begin{array}{rcl} \mathrm{Der}(\mathbb{F}_q(X)) & \longrightarrow & \mathbb{F}_q(X) \\ D & \longmapsto & D(X) \end{array}$$

est un isomorphisme de $\mathbb{F}_q(X)$-espaces vectoriels.
En déduire la dimension de $\mathrm{Der}(\mathbb{F}_q(X))$ sur $\mathbb{F}_q(X)$ et en donner une base explicite.

Partie III

Dans cette partie **III**, on fixe un corps différentiel (K, D) où K est de **caractéristique nulle**. Pour toute extension différentielle L de K, on note encore D la dérivation sur L qui prolonge celle de K et fait de L/K une extension différentielle.
Si $K = \mathbb{C}(X)$, on note $\partial(u)$ ou u' la dérivée usuelle d'un élément u appartenant à K ou à une extension différentielle de K.

Définitions. Si v appartient à une extension différentielle de K, on dit que :

— v est un *logarithme* d'un élément de K s'il existe $u \in K^*$ tel que $D(v) = \frac{D(u)}{u}$; dans ce cas, on dit que v est *un logarithme de* u ;

— v est une *exponentielle* d'un élément de K si $v \neq 0$ et s'il existe u dans K tel que $D(v) = D(u)v$; dans ce cas, on dit que v est *une exponentielle de* u.

Définitions. Soit $(L/K, D)$ une extension différentielle. Pour tous corps K_1, K_2 tels que : $K \subseteq K_1 \subseteq K_2 \subseteq L$, on dit que l'extension K_2/K_1 est :

— *logarithmique* s'il existe v dans K_2 tel que $K_2 = K_1(v)$, où v est un logarithme d'un élément de K_1 ;

— *exponentielle* s'il existe v dans K_2^* tel que $K_2 = K_1(v)$, où v est une exponentielle d'un élément de K_1.

Définition. Soit $(L/K, D)$ une extension différentielle. On dit que L est une extension *élémentaire* de K s'il existe un entier naturel m et une famille de corps $(K_i)_{0\leqslant i\leqslant m}$ vérifiant les propriétés suivantes :

— $K_0 = K$, $K_m = L$, et, pour tout i dans $[\![0, m-1]\!]$, $K_i \subseteq K_{i+1}$;

— pour tout i dans $[\![0, m-1]\!]$, l'extension de corps K_{i+1}/K_i est finie ou logarithmique ou exponentielle.

Nous **admettons** les propriétés suivantes, qui découlent de théorèmes généraux d'analyse complexe :

— pour toute fraction rationnelle R dans $\mathbb{C}(T)$, il existe une extension différentielle de $(\mathbb{C}(T), \partial)$ contenant une exponentielle de R, notée e^R ;

— pour toutes fractions rationnelles $R_1, \ldots, R_k \in \mathbb{C}(T) \setminus \{0_{\mathbb{C}(T)}\}$, il existe une extension différentielle de $(\mathbb{C}(T), \partial)$ contenant des logarithmes de $R_1, \ldots, R_k$, notés $\ln(R_1), \ldots, \ln(R_k)$.

Ces deux propriétés restent valables si l'on remplace $\mathbb{C}(T)$ par une extension élémentaire de $(\mathbb{C}(T), \partial)$.
On retient en particulier que par définition, pour tout $R \in \mathbb{C}(X)$,

$$(e^R)' = R'e^R, \quad \text{et,} \quad \text{si } R \neq 0,\ (\ln(R))' = \frac{R'}{R}.$$

III.1 – Transcendance des exponentielles et logarithmes.

Dans cette sous-partie, on étudie à quelle condition une exponentielle ou un logarithme d'un élément de K est transcendant sur K.

Soit $(L/K, D)$ une extension différentielle et v dans L^*.

29. On suppose que v est une exponentielle d'un élément u de K.

(a) Démontrer que, si v est algébrique sur K et si $n = \deg(\mu_v)$, alors

$$nD(u)\mu_v = D(u)X\mu_v' + \mu_v^D.$$

En déduire que v^n est un élément de K.

Indication : On pourra utiliser le coefficient constant du polynôme μ_v.

(b) Réciproquement, démontrer que s'il existe un entier strictement positif n tel que v^n est un élément de K, alors v est algébrique sur K.

On a ainsi démontré que v est transcendant sur K si et seulement si, pour tout entier n dans $\mathbb{N} \setminus \{0\}$, $v^n \notin K$.

30. Dans cette question, on se place dans $K = \mathbb{C}(T)$ muni de la dérivation usuelle.

(a) Soit $R \in \mathbb{C}(T) \setminus \mathbb{C}$. Démontrer qu'il n'existe pas S dans $\mathbb{C}(T)$ tel que $\frac{R'}{R} = S'$.
Indication : On pourra utiliser les décompositions en éléments simples des fractions rationnelles $\frac{R'}{R}$ et S.

(b) En déduire que pour tout $S \in \mathbb{C}(T) \setminus \mathbb{C}$, une exponentielle e^S est transcendante sur $\mathbb{C}(T)$.

31. On suppose que v est un logarithme d'un élément u de K^*. Démontrer que, si v est algébrique sur K, alors $v \in K$.

III.2 – Primitives élémentaires et théorème principal.

Définition. Soit $f \in K$. On dit que l'élément f admet une *primitive élémentaire sur* K s'il existe une extension élémentaire $(L/K, D)$ et un élément g dans L tels que $D(g) = f$.

La question suivante étudie un exemple.

32. Soit e^{iT} une exponentielle de iT pour la dérivation usuelle de $\mathbb{C}(T)$. On pose :

$$\cos(T) = \frac{1}{2}\left(e^{iT} + \frac{1}{e^{iT}}\right) \quad \text{et} \quad \sin(T) = \frac{1}{2i}\left(e^{iT} - \frac{1}{e^{iT}}\right).$$

(a) Démontrer que $\dfrac{1}{1+T^2}$ admet une primitive élémentaire sur $\mathbb{C}(T)$ (muni de ∂) et que $\dfrac{\sin(T)}{1+(\cos(T))^2}$ admet une primitive élémentaire sur $\mathbb{C}\left(e^{iT}\right)$.

(b) Si $\operatorname{Arctan}(\cos(T))$ désigne un élément d'une extension élémentaire dont la dérivée est :

$$(\operatorname{Arctan}(\cos(T)))' = \frac{\sin(T)}{1+(\cos(T))^2},$$

vérifier que $\sqrt{\operatorname{Arctan}(\cos(T))}$ appartient à une extension élémentaire de $(\mathbb{C}(T), \partial)$.

Définition. Soit $f \in K$. On dit que f est une *somme de Liouville dans* K s'il existe g dans K, un ensemble fini I (éventuellement vide) et deux familles $(c_i)_{i\in I}$ dans $(K_{\text{cst}})^I$, $(f_i)_{i\in I}$ dans $(K^*)^I$ tels que :

$$f = D(g) + \sum_{i\in I} c_i L_D(f_i),$$

où L_D est le morphisme de la question **14**.
L'objectif de la partie **III** est de démontrer le théorème suivant.

> **Théorème principal.** Si un élément f de K admet une primitive élémentaire sur K, alors f est une somme de Liouville dans K.

La clé de la démonstration réside dans le lemme suivant.

> **Lemme principal.** Soit $(L/K, D)$ une extension différentielle finie, ou logarithmique, ou exponentielle. Si un élément f de K est une somme de Liouville dans L, alors f est une somme de Liouville dans K.

33. Démontrer que le lemme principal implique le théorème principal.

Les questions **34** à **49** sont consacrées à la démonstration du lemme principal.

III.3 – Le lemme principal pour les extensions finies.

Soit $(L/K, D)$ une extension différentielle **finie** et f dans K. On suppose que f est une somme de Liouville dans L. Soit g dans L et $(c_i)_{i\in I}$ dans $(L_{\text{cst}})^I$, $(f_i)_{i\in I}$ dans $(L^*)^I$ tels que $f = D(g) + \sum\limits_{i\in I} c_i L_D(f_i)$.

Soit P un polynôme unitaire non constant de $K[X]$ et soit M son corps de décomposition.

34. Soit $x \in M$. Démontrer que x est annulé par un polynôme de $K[X]$ scindé sur M, et en déduire que toutes les racines de $\mu_{x,K}$ sont dans M.
On pourra librement utiliser le théorème suivant :

> **Théorème fondamental des fractions symétriques.** Soit A un anneau commutatif et $R \in A(X_1, \dots, X_n)$. Soit $\Sigma_1, \dots, \Sigma_n$ les fonctions symétriques élémentaires en $X_1, \dots, X_n$ dans $A[X_1, \dots, X_n]$ définies par l'égalité :
>
> $$\prod_{i=1}^{n}(X - X_i) = X^n + \sum_{i=1}^{n}(-1)^i \Sigma_i X^{n-i}.$$
>
> On suppose :
>
> $$\forall \sigma \in \mathfrak{S}_n, \quad R(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = R(X_1, \dots, X_n),$$
>
> où $\mathfrak{S}_n$ désigne le groupe des permutations de $[\![1, n]\!]$.
> Alors il existe Q dans $A(X_1, \dots, X_n)$ tel que $R = Q(\Sigma_1, \dots, \Sigma_n)$.

Dans les questions **35** à **37**, on fixe un élément x de M. On note : $\mu_{x,K} = \sum_{i=0}^{n} a_i X^i$, avec les a_i dans K. Pour tout morphisme σ défini d'un surcorps de K dans M, on note $\mu_{x,K}^{\sigma} = \sum_{i=0}^{n} \sigma(a_i) X^i$.

35. Démontrer que si $\sigma : K(x) \to M$ est un morphisme de corps, alors $\sigma(x)$ est une racine du polynôme $\mu_{x,K}^{\sigma}$.

36. Soit τ un morphisme de corps de K dans M ; on note K^{τ} l'image de τ. Démontrer que, pour toute racine y de $\mu_{x,K}^{\tau}$, prise dans le corps de décomposition sur K^{τ} de ce polynôme, il existe un unique morphisme de corps σ de $K(x)$ dans $K^{\tau}(y)$ envoyant x sur y et qui prolonge τ.

37. Soit y une racine de $\mu_{x,K}$ dans M. Démontrer qu'il existe exactement $\dim_{K(x)}(M)$ automorphismes σ de $\mathrm{Aut}_K(M)$ tels que $\sigma(x) = y$.

38. En déduire :

$$\forall x \in M, \quad \mathrm{tr}_{M/K}(x) = \sum_{\sigma \in \mathrm{Aut}_K(M)} \sigma(x), \qquad \text{et} \qquad \mathrm{N}_{M/K}(x) = \prod_{\sigma \in \mathrm{Aut}_K(M)} \sigma(x).$$

39. On suppose dans cette question que M est le corps de décomposition de $\mu_{g,K} \cdot \prod_{i \in I} \mu_{f_i,K}$ sur K. Déduire de tout ce qui précède :

$$\forall i \in I, \ \mathrm{tr}_{M/K}\left(L_D(f_i)\right) = L_D\left(\mathrm{N}_{M/K}(f_i)\right), \qquad \text{et} \qquad \mathrm{tr}_{M/K}\left(D(g)\right) = D\left(\mathrm{tr}_{M/K}\left(g\right)\right),$$

puis que f est une somme de Liouville dans K.

III.4 – Le lemme principal pour les extensions logarithmiques ou exponentielles.

On ne suppose plus que L/K est finie. On suppose que l'extension L/K est **logarithmique** ou **exponentielle**. Soit v un élément de L tel que $L = K(v)$ et u un élément de K tel que $D(v) = \frac{D(u)}{u}$ si L/K est logarithmique, et tel que $D(v) = D(u)v$ si L/K est exponentielle.

40. Justifier qu'on peut supposer sans perte de généralité que v est transcendant sur K. En déduire l'existence d'un isomorphisme de K-algèbres $\Phi : K(X) \to L$ dont la restriction à K est l'identité, et d'une extension différentielle $(K(X)/K, D_1)$, tels que $\Phi \circ D_1 = D \circ \Phi$, et vérifiant :

$$D_1(X) = \frac{D(u)}{u} \text{ (cas logarithmique)}, \qquad \text{ou} \qquad \frac{D_1(X)}{X} = D(u) \text{ (cas exponentiel)}.$$

Nous dirons que D_1 est une dérivation *logarithmique* dans le premier cas et que c'est une dérivation *exponentielle* dans le second. On pose $\alpha = D_1(X)$ dans le cas logarithmique et $\alpha = \frac{D_1(X)}{X}$ dans le cas exponentiel. On remarque que α est un élément de K.

Soit $f \in K$. On suppose que f est une somme de Liouville dans L.

41. Démontrer que f est une somme de Liouville dans $K(X)$ (muni de la dérivation D_1 de la question **40**).

42. Démontrer qu'il existe R dans $K(X)$, $(R_i)_{i \in I}$ dans $(K(X)^*)^I$, $(c_i)_{i \in I}$ dans K_{cst}^I (où I est un ensemble fini, éventuellement vide) avec les c_i **non nuls et linéairement indépendants sur** $\mathbb{Q}$, tels que

$$f = D_1(R) + \sum_{i \in I} c_i L_{D_1}(R_i).$$

43. Expliciter un corps de décomposition sur K, noté M, sur lequel f peut s'écrire :

$$f = D_1(P) + \sum_{(j,s)\in J\times S} D_2\left(\frac{n_{j,s}}{(X-\lambda_j)^s}\right) + \sum_{i\in I} c_i L_{D_1}(a_i) + \sum_{(i,j)\in I\times J} c_i m_{i,j} \frac{D_1(X) - D_2(\lambda_j)}{X-\lambda_j}$$

où D_2 est l'unique prolongement de D_1 en une dérivation de $M(X)$ et

— les ensembles I, J et S sont des parties finies de $\mathbb{N}\setminus\{0\}$ (éventuellement vides) ;

— les $n_{j,s}$ et les λ_j sont dans M, les λ_j étant **distincts deux à deux** ;

— les c_i sont dans K^*_{cst} et $\mathbb{Q}$-**linéairement indépendants**, et les a_i dans K^* ;

— les $m_{i,j}$ sont des entiers relatifs ;

— le polynôme P est dans $K[X]$.

44. Soit $j \in J$. Démontrer que la fraction $\frac{D_1(X)-D_2(\lambda_j)}{X-\lambda_j}$ de $M(X)$ vérifie selon les cas :

— si D_1 est exponentielle et $\lambda_j = 0$, $\frac{D_1(X)-D_2(\lambda_j)}{X-\lambda_j} \in K$;

— sinon, $\frac{D_1(X)-D_2(\lambda_j)}{X-\lambda_j}$ est non nulle et sous forme irréductible.

Indication : Pour cela, on pourra raisonner par l'absurde et utiliser la fonction $\mathrm{tr}_{M/K}$. On procédera alors en deux temps :

— si D_1 est logarithmique, démontrer qu'il existe β dans K, tel que $X-\beta$ appartienne à K_{cst}, puis conclure ;

— si D_1 est exponentielle et si $\lambda_j \neq 0$, démontrer qu'il existe n dans $\mathbb{N}\setminus\{0\}$ et u dans K^* tels que $n\alpha = L_{D_1}(u)$, puis conclure.

45. Par une étude analogue, démontrer que si $n_{j,s} \neq 0$ alors le plus grand exposant de $\frac{1}{X-\lambda_j}$, dans la décomposition en éléments simples de $D_2\left(\frac{n_{j,s}}{(X-\lambda_j)^s}\right)$, est supérieur ou égal à 2, sauf éventuellement si D_1 est exponentielle et $\lambda_j = 0$.

Démontrer que dans ce cas exceptionnel, si $n_{j,s} \neq 0$ alors le plus grand exposant de $\frac{1}{X}$ dans la décomposition en éléments simples de $D_2\left(\frac{n_{j,s}}{X^s}\right)$ est égal à s.

46. Démontrer que $D_1(P) \in K[X]$. En déduire que $n_{j,s} = 0$ pour tout $(j,s) \in J\times S$, puis que $m_{i,j} = 0$ pour tout $(i,j) \in I\times J$ sauf éventuellement si D_1 est exponentielle et $\lambda_j = 0$.

47. On suppose D_1 logarithmique. Démontrer que si $D_1(P)$ est un polynôme constant, alors P est de degré au plus 1 et son coefficient dominant est dans K_{cst}.

48. On suppose D_1 exponentielle. Démontrer que si $D_1(P)$ est un polynôme constant, alors P l'est également.

Donner également une condition nécessaire sur le degré de P pour que $D_1(P)$ soit de degré au plus 1.

49. Conclure en démontrant que f est une somme de Liouville dans K.

On a ainsi démontré le lemme principal dans tous les cas. Par la question **33**, le théorème principal est démontré.

III.5 – Primitives élémentaires de fe^g et de $\frac{\ln(T)}{T-\lambda}$.

La fin du sujet est consacrée à une application du théorème principal à l'étude des primitives d'un élément de la forme fe^g ou $\frac{\ln(T)}{T-\lambda}$.

50. Soit D une dérivation exponentielle sur $K(X)$. Soit $f \in K$. Déduire de ce qui précède que Xf est une somme de Liouville dans $K(X)$ si et seulement s'il existe a dans K tel que $Xf = D(aX)$.

51. Soit $f \in \mathbb{C}(T)$ et $g \in \mathbb{C}(T) \setminus \mathbb{C}$. Démontrer que l'élément fe^g admet une primitive élémentaire sur $\mathbb{C}(T)(e^g)$ (pour la dérivation usuelle) si et seulement s'il existe une fraction rationnelle b de $\mathbb{C}(T)$ telle que $f = b' + bg'$.

52. Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Démontrer que

$$e^{T^n} \quad \text{et} \quad \frac{e^T}{T}$$

n'admettent pas de primitive élémentaire sur $\mathbb{C}(T)\left(e^{T^n}\right)$ et respectivement $\mathbb{C}(T)\left(e^{T}\right)$ pour la dérivation usuelle.

53. Soit $\lambda \in \mathbb{C}$. En s'inspirant des questions précédentes, donner une condition nécessaire et suffisante simple sur λ pour que

$$\frac{\ln(T)}{T - \lambda}$$

admette une primitive élémentaire sur $\mathbb{C}(T)\left(\ln(T)\right)$ pour la dérivation usuelle.