Agrégation Externe de Mathématiques 2025
Mathématiques Générales : proposition de corrigé

J. Le Borgne

Exercice

1. Le polynôme $X^3-2 \in \mathbf{Z}[X]$ vérifie le critère d'Eisenstein relativement au nombre premier 2 (son coefficient dominant est impair, tous ses coefficients sont pairs, et son coefficient constant n'est pas divisible par 4), ce qui assure que ce polynôme est irréductible dans $\mathbf{Q}[X]$. Alternativement, on peut remarquer que ce polynôme de degré 3 n'a pas de racine rationnelle ($\sqrt[3]{2}$ est irrationnel, et les autres racines complexes de ce polynôme ne sont pas réelles) ce qui assure aussi qu'il est irréductible.

2. La question 1. montre que $\mathrm{Ann}_{\sqrt[3]{2},\mathbf{Q}} = (X^3-2)$. Soit $(a,b,c) \in \mathbf{Q}^3$ tel que $a\sqrt[3]{4}+b\sqrt[3]{2}+c=0$, alors $aX^2+bX+c \in \mathrm{Ann}_{\sqrt[3]{2},\mathbf{Q}}$, donc divisible par X^3-2, et donc nul : $a=b=c=0$. En particulier, la famille $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ est libre. D'autre part, soit $P \in \mathbf{Q}[X]$, par division euclidienne par X^3-2, on peut écrire $P = Q(X)(X^3-2)+(aX^2+bX+c)$ avec $Q \in \mathbf{Q}[X]$ et $a,b,c \in \mathbf{Q}$. En évaluant en $\sqrt[3]{2}$, il vient $P(\sqrt[3]{2}) = a\sqrt[3]{4}+b\sqrt[3]{2}+c$. Ainsi, la famille $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ engendre le $\mathbf{Q}$-espace vectoriel $Q[\sqrt[3]{2}]$. C'est bien une base de $Q[\sqrt[3]{2}]$.

3. Par un calcul direct, la matrice de m_α dans cette base est : $\begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$.

4. Le calcul du polynôme caractéristique de la matrice précédente donne $\chi_{m_\alpha} = X^3-3X^2-3X-1$.

5. On a $\chi'_{m_\alpha} = 3(X^2-2X-1)$, et $X^3-3X^2-3X-1 = (X-1)(X^2-2X-1)-4X-1$, donc $\mathrm{pgcd}(\chi_{m_\alpha}, \chi'_{m_\alpha}) = \mathrm{pgcd}(X^2-2X-1, 4X+1) = 1$. En particulier, χ_{m_α} est sans facteurs carrés, or les facteurs irréductibles de π_{m_α} dans $\mathbf{Q}[X]$ sont ceux de χ_{m_α}, donc $\pi_{m_\alpha} = \chi_{m_\alpha}$.

Problème

Partie I

1. a) L'anneau $K[x]$ est une K-algèbre et $x \in K[x]$. Par propriété universelle de $K[X]$, il existe un unique morphisme de K-algèbres $\Phi : K[X] \to K[x]$ tel que $\Phi(X) = x$ (ce morphisme envoie un polynôme P sur $P(x)$). Par définition d'un morphisme de K-algèbres, sa restriction à K est l'identité. Par définition,

$$\ker \Phi = \{P \in K[X] \text{ tels que } P(x)=0\} = \mathrm{Ann}_{x,K}.$$

b) Supposons x transcendant, alors $\mathrm{Ann}_{x,K} = \{0\}$ donc Φ est injectif. Par définition de $K[x]$, il est surjectif. C'est donc un isomorphisme de K-algèbres. En particulier, Φ induit un isomorphisme entre leurs corps de fractions, c'est-à-dire entre $K(X)$ et $K(x)$.

En particulier, le K-espace vectoriel $K(x)$ a la même dimension que $K(X)$, et $K(X)$ est de dimension infinie sur K car la famille $\{\frac{1}{(X-\lambda)^n},\ \lambda \in K, n \in \mathbf{N}^*\}$ est libre sur K par le théorème de décomposition en élément simples.

c) Si x est algébrique, alors Φ induit un isomorphisme de K-algèbres $K[X]/(\mu_x) \to K[x]$ (la surjectivité suit encore de la définition de $K[x]$). Comme μ_x est irréductible, ce quotient est un corps, donc $K[x]$ aussi, et donc $K(x) = K[x]$. La famille $(1, X, \dots, X^{\deg \mu_x - 1})$ (ou plutôt son image par la projection caononique $K[X] \to K[X]/(\mu_x)$) est une base de $K[X]/(\mu_x)$. En effet, le théorème de division euclidienne assure qu'elle est génératrice, et la minimalité de μ_x assure qu'elle est libre. En particulier,$K(x)$ est de dimension $\deg \mu_x$, avec pour base l'image par Φ de la base précédente, c'est-à-dire $(1, x, \dots, x^{\deg \mu_x - 1})$.

2. Supposons que μ_x admette une racine au moins double α, en particulier $\mu_x(\alpha) = 0$. Comme μ_x est irréductible et unitaire, $\mu_\alpha = \mu_x$. Si $\mu_x' \neq 0$, alors $\deg \mu_x' < \deg \mu_\alpha$ et $\mu_x'(\alpha) = 0$ contredit la minimalité de μ_x. Donc $\mu_x' = 0$.

3. Soit $P = \sum_{i=0}^n a_i X^i \in K[X]$, alors $P' = \sum_{i=0}^n i a_i X^{i-1}$. Ainsi, $P' = 0$ si et seulement si pour tout $i \geq 0$, $ia_i = 0$. Si K est de caractéristique 0, cette condition équivaut à $a_i = 0$ pour tout $i \neq 0$; si K est de caractéristique P, cette condition équivaut à $a_i = 0$ pour tout $i \notin p\mathbf{N}$. Autrement dit :
— si K est de caractéristique 0, $P' = 0$ si et seulement si P est constant ;
— si K est de caractéristique $p > 0$, $P' = 0$ si et seulement si P est de la forme $P(X) = Q(X^p)$ pour un certain $Q \in K[X]$.
La question 2 montre alors que si K est de caractéristique 0, μ_x est à racines simples. Si K est fini de caractéristique $p > 0$, l'application $x \mapsto x^p$ est un endomorphisme de l'anneau K (valable pour tout anneau commutatif de caractéristique p, en utilisant la formule du binôme de Newton) qui est surjectif car c'est une application injective entre ensembles finis (tout morphisme d'anneaux unitaires défini sur un corps K est injectif car ses idéaux sont $\{0\}$ et K, et le noyau d'un tel morphisme est un idéal différent de K). Dans ce cas, la description précédente des polynômes de dérivée nulle se reformule de la manière suivante : si K est fini de caractéristique $p > 0$, $P' = 0$ si et seulement si P est de la forme $Q(X)^p$ pour un certain $Q \in K[X]$. Comme $p \geq 2$, aucun polynôme de cette forme n'est irréductible, donc $\mu_x' \neq 0$. D'après la question 2, μ_x est à racines simples.

4. Soient $x, x' \in L$ et $\lambda \in K$. Soit $y \in L$, alors $m_{\lambda x + x'}(y) = (\lambda x + x')y = \lambda xy + x'y = \lambda m_x(y) + m_{x'}(y)$, donc $m \mapsto m_x$ est linéaire. De plus, $m_{xx'}(y) = xx'y = m_x \circ m_{x'}(y)$, et $m_1 = \mathrm{Id}_L$, donc $x \mapsto m_x$ est un morphisme de K-algèbres. En particulier, si $x \neq 0$, m_x est inversible d'inverse $m_{x^{-1}}$: cela montre l'injectivité de $x \mapsto m_x$. Cette application étant un morphisme de K-algèbres, on a pour tout $P \in K[X]$ $m_{P(x)} = P(m_x)$. Par injectivité, $m_{P(x)} = 0$ si et seulement si $P(x) = 0$, donc $P(m_x) = 0$ si et seulement si $P(x) = 0$: x et m_x ont le même idéal annulateur, donc x est algébrique si et seulement si m_x admet un polynôme annulateur, et dans ce cas le polynôme minimal de m_x est μ_x.

5. Munissons $K(x)$ de la base $(1, x, \dots, x^{d-1})$ établie en 1.c). La matrice de m_x dans cette base est C, car $x \cdot x^i = x^{i+1}$ si $0 \leq i \leq d-2$, et $x \cdot x^{d-1} = x^d = -a_0 - a_1 x - \dots - a_{d-1}x^{d-1}$.

6. Soit $x \in L$. Par définition, $\mathrm{tr}_{L/K}(x)$ et $N_{L/K}(x)$ sont respectivement la trace et le déterminant de l'endomorphisme m_x du K-espace vectoriel de dimension finie L. Ce sont donc des éléments de K.

7. a) D'après la question 4, l'application $x \mapsto m_x$ est un morphisme de K-algèbres de L dans $\mathcal{L}_K(L)$. En particulier, $\mathrm{tr}_{L/K}$ est linéaire comme composée d'applications linéaires, et $N_{L/K}$ est multiplicative comme composée d'applications multiplicatives.
En outre, si $x \in L^\times$, alors toujours par la question 4, m_x est un isomorphisme. Donc son déterminant est non nul, ce qui donne exactement $N_{L/K}(x) \neq 0$.

b) Soit $u \in K$, alors l'application m_u est l'homothétie de rapport u. En particulier, $\mathrm{tr}_{L/K}(u) = \dim_K(L)u$ et $N_{L/K}(u) = u^{\dim_K(L)}$.

8. Comme L est un K-espace vectoriel de dimension finie, la famille $\{x^n, n \in \mathbf{N}\}$ est finie ou liée. Si elle est finie alors on dispose de $m, n \in \mathbf{N}$ distincts tels que $x^m = x^n$, donc x est algébrique sur K. Si elle est liée, alors on dispose de $a_0, \dots, a_n \in K$ non tous nuls tels que $a_0 + a_1 x + \cdots + a_n x^n = 0$, donc x est algébrique sur K (avec comme polynôme annulateur $a_0 + a_1 X + \cdots + a_n X^n$).

9. Soit $y \in L$, on peut écrire $y = \sum_{i=1}^{a} \alpha_i \ell_i$ avec $\alpha_i \in K(x)$ pour tout $1 \leq i \leq a$. D'après la question 1.c), on peut écrire pour tout $1 \leq i \leq a$, $\alpha_i = \sum_{j=10}^{d-1} \lambda_{i,j} x^j$ avec $\lambda_{i,j} \in K$. La famille considérée est donc génératrice. Par multiplicativité des degrés (résultat rappelé dans l'énoncé), le cardinal de cette famille est la dimension du K-espace vectoriel L ; c'est bien une base de L.

10. On considère la base de la question précédente, en l'ordonnant de sorte que $\ell_i x^j \leq \ell_{i'} x^{j'}$ si et seulement si $i < i'$ ou $i = i'$ et $j \leq j'$. Chacun des sous-espaces $\ell_i K(x)$ est stable par multiplication par x, et dans cette base, la matrice de m_x est diagonale par blocs avec comme unique bloc diagonal la matrice C (qui est la matrice de l'endomorphisme de multiplication par x dans la base choisie sur chacun des $\ell_i K(x)$ par la question 5).
La forme de la matrice assure alors que $\mathrm{tr}_{L/K}(x) = \frac{n}{d}\mathrm{Tr}(C)$ et $N_{L/K}(x) = \det(C)^{\frac{n}{d}}$. Comme C est la matrice compagnon de μ_x, ses valeurs propres sont les racines de μ_x et on a $\mathrm{Tr}(C) = x_1 + \cdots + x_d$ et $\det(C) = x_1 \cdots x_d$, ce qui démontre le résultat voulu.

Partie II

II.1 - Formulaire de calcul

11. On a $D(1^2) = D(1) + D(1)$ d'où $D(1) = 0$. Soit $x \in K^\times$. Par définition, $0 = D(xx^{-1}) = xD(1/x) + D(x)/x$. On a donc $D\left(\frac{1}{x}\right) = -\frac{D(x)}{x^2}$.

12. Démontrons la première relation par récurrence sur $n \in \mathbf{N}^*$ (elle est aussi vraie pour $n = 0$) : si $n = 1$, la relation est simplement $D(x) = D(x)$, qui est vraie. Supposons que pour un $n \in \mathbf{N}^*$, $D(x^n) = nx^{n-1}D(x)$. Alors $D(x^{n+1}) = D(x^n x) = x \times nx^{n-1}D(x) + x^n D(x) = (n+1)x^n D(x)$, qui est bien la relation voulue au rang $n+1$.
Pour la deuxième relation, soient $x, y \in K$. On a $D(xy^{-1}) = xD(y^{-1}) + y^{-1}D(x) = -xy^{-2}D(y) + y^{-1}D(x) = y^{-2}(yD(x) - xD(y))$ d'après la question 11.
Enfin, si on suppose $x \neq 0$, et si $n \in \mathbf{N}^*$,

$$D(x^{-n}) = D((x^{-1})^n) = n(x^{-1})^{n-1}D(x^{-1}) = -nx^{-n-1}D(x).$$

Cela démontre la relation voulue pour les entiers négatifs.

13. Par $\mathbf{Z}$-linéarité de D, K_{cst} est un sous-groupe de K. De plus d'après 11. on a $1 \in K_{\mathrm{cst}}$ et si $x, y \in K_{\mathrm{cst}}$ alors $D(xy) = 0$ d'où $xy \in K_{\mathrm{cst}}$. Enfin, si $x \in K_{\mathrm{cst}}$, alors $D(x^{-1}) = x^{-2}D(x) = 0$ donc $x^{-1} \in K_{\mathrm{cst}}$. Cela montre que K_{cst} est un sous-corps de K.
Soit $\lambda \in K_{\mathrm{cst}}$ et soit $x \in K$, on a $D(\lambda x) = \lambda D(x) + xD(\lambda) = \lambda D(x)$. Cela montre que D est K_{cst}-linéaire, car on sait déjà qu'elle est $\mathbf{Z}$-linéaire.

14. a) On a $L_D(1) = D(1)/1 = 0$. Soient $x, y \in K^\times$, alors $L_D(xy^{-1}) = x^{-1}yD(xy^{-1}) = D(x)/x - D(y)/y = L_D(x) - L_D(y)$. Cela montre que L_D est un morphisme de groupes. Par définition, $\ker L_D = K_{\mathrm{cst}}^\times$.

b) D'après la question précédente, on a $L_D(R) = L_D(c) + \sum_{i=1}^{r} \beta_i L_D(X - \alpha_i)$, ce qui est exactement la relation voulue.

II.2 - Construction de dérivations

15. Le polynôme $X^2+X+1 \in \mathbf{F}_2[X]$ est irréductible car il n'a pas de racines et est de degré 2. Soit j la classe de X dans $L = \mathbf{F}_2[X]/(X^2+X+1)$. Alors $L = \mathbf{F}_4$ (à isomorphisme près) et $L = \mathbf{F}_2(j)$. On a $j^3 = 1$ donc $D(j^3) = 0$. Par ailleurs, $D(j^3) = 3j^2D(j)$ donc $D(j) = 0$, et $D(j^2) = 2jD(j) = 0$. Par linéarité, $D = 0$.

16. Soit D une dérivation sur $\mathbf{F}_q$, et soit $x \in \mathbf{F}_q^\times$. Alors $x^{q-1} = 1$ donc $0 = (q-1)x^{q-2}D(x) = -D(x)/x$. On a donc $D(x) = 0$. Cela montre que l'application nulle est la seule dérivation de $\mathbf{F}_q$.

17. L'application D' est bien définie car Φ est un isomorphisme. C'est un endomorphisme du groupe $(K,+)$ comme composée des morphismes de groupes Φ, D et Φ^{-1}. Soient $x', y' \in K'$, alors $D'(x'y') = \Phi^{-1}(\Phi(x')D(\Phi(y')) + \Phi(y')D(\Phi(x))) = x'D'(y) + y'D'(x)$ car Φ est un morphisme de corps et D est une dérivation. Donc D' est une dérivation
Enfin, par injectivité de Φ^{-1}, $D'(x') = 0$ si et seulement si $\Phi(x') \in K_{\text{cst}}$: on a donc bien $K'_{\text{cst}} = \Phi^{-1}(K_{\text{cst}})$.

18. Soit D une dérivation sur A. Supposons que D se prolonge à B en une dérivation $\widehat{D}$, alors pour tout $(a,b) \in A \times (A \setminus \{0\})$, on a $\widehat{D}\left(\frac{a}{b}\right) = b^{-2}(D(a)b - aD(b))$. Cela montre que D se prolonge d'au plus une manière en une dérivation de B. Vérifions que la formule précédente définit bien une dérivation sur B. Montrons d'abord que le résultat obtenu par cette formule de calcul ne dépend pas du choix du représentant pour $\frac{a}{b}$: soient $a' = \lambda a$ et $b' = \lambda b$ avec $\lambda \in A \setminus \{0\}$, alors dans B,

$$\begin{aligned}(\lambda b)^{-2}(D(\lambda a)\lambda b - \lambda a D(\lambda b)) &= (\lambda b)^{-2}(D(\lambda)a\lambda b + \lambda^2 D(a)b - \lambda a D(\lambda)b - \lambda a D(\lambda)b)\\ &= b^{-2}(D(a)b - D(b)a).\end{aligned}$$

Cela montre que cette formule définit bien une fonction $\widehat{D}$ sur B. Soient $x, x' \in B$, écrivons $x = \frac{a}{q}$ et $x' = \frac{a'}{q}$ avec $a, a' \in A$ et $q \in A \setminus \{0\}$, ce que l'on peut supposer quitte à réduire au même dénominateur. On a alors $x + x' = \frac{a+a'}{q}$, de sorte que $\widehat{D}(x+x') = q^{-2}(D(a+a')q + (a+a')D(q)) = \widehat{D}(x) + \widehat{D}(x')$.
D'autre part, $xx' = \frac{aa'}{q^2}$, on a donc $\widehat{D}(xx') = q^{-4}(D(aa')q^2 - aa'D(q^2)) = q^{-4}(aD(a')q^2 + a'D(a)q^2 - 2aa'qD(q))$. Après simplification, il vient $\widehat{D}(xx') = q^{-1}(xD(a') + x'D(a) - 2xx'D(q)) = x\widehat{D}(x') + x'\widehat{D}(x)$, car $\widehat{D}(x) = q^{-1}(D(a) + xD(q))$ (et même chose pour $\widehat{D}(x')$ *mutatis mutandis*). L'application $\widehat{D}$ ainsi définie vérifie donc bien la relation de Leibniz, et c'est l'unique dérivation qui prolonge D à B.

19. Comme $K(x) = \text{Frac}(K[x])$, il suffit d'appliquer la question 18. avec $A = K[x]$ muni de la dérivation $D(P) = P^D$, sous réserve de démontrer que cette application soit bien une dérivation. Il est clair que c'est un endomorphisme de $(K[x],+)$. Soient $i, j \in \mathbf{N}$ et $a, b \in K$. Alors $(ax^ibx^j)^D = D(ab)x^{i+j} = (ax^i)(bx^j)^D + (ax^i)^D(bx^j)$; par $\mathbf{Z}$-linéarité, $P \mapsto P^D$ est bien une dérivation de $K[x]$ et elle se prolonge donc de manière unique en une dérivation de $K(x)$.

20. Comme K est de caractéristique 0, $\mu_x' \neq 0$ donc $\text{pgcd}(\mu_x, \mu_x') = 1$, c'est-à-dire que l'idéal engendré par μ_x et μ_x' est $K[X]$. On dispose donc en particulier de $P, Q \in K[X]$ tels que $P\mu_x - Q\mu_x' = \mu_x^D$. Après évaluation en x il vient $\mu_x^D(x) + Q(x)\mu_x'(x) = 0$.

21. Il suffit de vérifier que pour tout $P \in \mu_x K[X]$, $P^D(x) + Q(x)P'(x) = 0$. Écrivons $P = A\mu_x$, alors $P^D + QP' = A\mu_x^D + A^D\mu_x + QA\mu_x' + QA'\mu_x$. En évaluant en x, on obtient bien $P^D(x) + Q(x)P'(x) = A(\mu_x^D(x) + Q(x)\mu_x'(x)) = 0$.
Ainsi, l'application linéaire $\varphi : K[X] \to K[X]/\mu_x K[X]$ définie par $P \mapsto P^D + QP'$ vérifie $\mu_x K[X] \subset \ker\varphi$. Par propriété universelle du quotient, il existe une unique application

linéaire $\bar{\varphi} : L = K[X]/\mu_x K[X] \to K[X]/\mu_x K[X]$ telle que $\bar{\varphi}(\bar{P}) = \varphi(P)$ (si on note $\bar{P}$ la classe de P modulo μ_x). La restriction de cette application à K est D car pour tout $\lambda \in K$, $\lambda' = 0$.

22. Notons que l'ensemble des dérivations sur $K(x)$ est un sous-espace vectoriel de l'espace des endomorphismes de groupe de $K(x)$. Ainsi, il suffit de démontrer que si D est une dérivation sur $K(x)$ telle que $D_{|K} = 0$, on a $D = 0$. Soit D une telle dérivation. Soit $\pi_x = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. On a $\pi_x(x) = 0$ donc $D(\pi_x(x)) = 0$. Ainsi, comme on a supposé $D_{|K} = 0$, on a $a_0 D(x) + a_1 D(x^2) + \cdots + a_{n-1} D(x^{n-1} + D(x^n) = 0$, donc $\mu_x'(x) D(x) = 0$. En particulier, comme $\mu_x'(x) \neq 0$, $D(x) = 0$ et donc $D(x^k) = k x^{k-1} D(x) = 0$ pour tout $k \in \mathbf{N}$. On en déduit que $D = 0$, d'où l'unicité voulue.

23. Démontrons le résultat par récurrence sur $n = \dim_K(L)$. Notre hypothèse de récurrence au rang n est la suivante : *Soit (K, D) un corps différentiel, soit L/K une extension finie de degré n, alors il existe une unique dérivation $\widehat{D} : L \to L$ telle que $\widehat{D}$ prolonge D.*
Initialisation. Si $n = 1$, alors $K = L$ donc il existe bien un unique prolongement, $\widehat{D} = D$.
Hérédité. Soit $n \geq 2$. Supposons le résultat vrai pour les extensions de degré $< n$. Supposons $[L : K] = n$. On dispose de $x \in L$ tel que $x \notin K$. On a donc $K \subset K_1 = K(x) \subset L$, et la première inclusion est stricte. D'après la question 21, D se prolonge à K_1 en une dérivation D_1, et ce prolongement est unique d'après la question 22. Par hypothèse de récurrence, appliquée à l'extension L du corps différentiel (K_1, D_1) (on a bien $[L : K_1] < n$), la dérivation D_1 se prolonge de manière unique à L en une dérivation $\widehat{D}$. Cette dérivation est un prolongement de D. C'est le seul prolongement de D en une dérivation, car si $\tilde{D}$ est une dérivation prolongeant de D à L, alors $\tilde{D}_{|K_1} = D_1$ par unicité de D_1 et donc $\tilde{D} = \widehat{D}$ par unicité de $\widehat{D}$.

24. On applique directement le résultat suivant : l'extension L/K est finie si et seulement si elle est engendrée par un nombre fini d'éléments algébriques sur K. On a donc par hypothèse $L = K(x_1, \ldots, x_n)$ pour $x_1, \ldots, x_n \in L$ algébriques sur K. Vus comme éléments de $L(X)$, ils sont algébriques sur $K(X)$, et $L(X) = K(X)(x_1, \ldots, x_n)$ donc $L(X)$ est un $K(X)$-espace vectoriel de dimension finie. Pour détailler un peu, l'implication réciproque (un extension engendrée par un nombre fini d'éléments algébriques est algébrique) qui constitue la partie difficile de ce résultat peut se démontrer par récurrence sur le nombre de générateurs, en utilisant la formule de multiplicativité des degrés et le cas intermédiaire $L = K(x)$ comme dans la question 23.
Le résultat de la question 23 s'applique : toute dérivation de $K(X)$ s'étend de manière unique à $L(X)$.

25. Soit $K/\mathbf{Q}$ une extension finie. Soit D une dérivation de K. Comme $D(1) = 0$, on a $D(k) = 0$ pour tout $k \in \mathbf{N}$ (par récurrence sur k) puis $D(\mathbf{Z}) = \{0\}$ et finalement $D(\mathbf{Q}) = 0$ en utilisant la formule pour $D(a/b)$ lorsque a, b sont entiers. Ainsi, la restriction de D à $\mathbf{Q}$ est la dérivation nulle, et D est l'unique prolongement de $\mathbf{Q}$ à K de cette dérivation : D est la dérivation nulle.

26. Soit $\sigma : L \to L$ un automorphisme K-linéaire. D'après la question 17, $\sigma^{-1} \circ D \circ \sigma$ est une dérivation de L. De plus, si $x \in K$ alors $\sigma^{-1} \circ D \circ \sigma(x) = \sigma^{-1}(D(x)) = D(x)$ car $D(x) \in K$ par hypothèse. Ainsi, la restriction de $\sigma^{-1} \circ D \circ \sigma$ à K est D. D'après la question 23, D est l'unique prolongement de $\sigma^{-1} \circ D \circ \sigma$ en une dérivation de L , on a donc $D = \sigma^{-1} \circ D \circ \sigma$ d'où $\sigma \circ D = D \circ \sigma$.

27. Soit $K = \mathbf{F}_q(X^q) \subset L = \mathbf{F}_q(X)$. Soit $P \in K[T]$ le polynôme $P(T) = T^q - X^q$, alors $X \in L$ est racine de P, donc X est algébrique sur K. En particulier $L = K(X)$ est une extension finie de K (le critère d'Eisenstein appliqué à $P \in \mathbf{F}_q[X^q][T]$ avec l'idéal (X^q) montre en fait que P est irréductible dans $K[T]$, donc que c'est le polynôme minimal de X).
Considérons maintenant la dérivation usuelle sur L ; elle est non nulle car $(X)' = 1$.

Soit $f \in K$, écrivons $f = g(X^q)$ avec $g \in \mathbf{F}_q(X)$, alors $f' = qX^{q-1}g'(X^q) = 0$ car K est de caractéristique p. Ainsi, la dérivation usuelle et la dérivation nulle de L sont des dérivations distinctes prolongeant la dérivation nulle sur K.

28. L'application considérée est bien définie, et clairement $\mathbf{F}_q(X)$-linéaire.
Soit D une dérivation sur $\mathbf{F}_q(X)$. Le même raisonnement qu'à la question 16 montre que $D_{|\mathbf{F}_q} = 0$. En particulier, si $A = \sum_{i=0}^{n} a_i X^i \in \mathbf{F}_q[X]$ alors $D(A) = \sum_{i=0}^{n} i a_i X^{i-1} D(X) = D(X)A'$. La formule pour la dérivation du quotient montre alors immédiatement que pour tout $f \in \mathbf{F}_q(X)$, $D(f) = D(X)f'$. En particulier, $D = D(X)\frac{d}{dX}$, où $\frac{d}{dX}$ désigne la dérivation usuelle.
Ainsi, l'application $D \mapsto D(X)$ est un isomorphisme $\mathbf{F}_q(X)$-espaces vectoriels, de réciproque $f \mapsto f\frac{d}{dX}$. On en déduit que la famille $\left\{\frac{d}{dX}\right\}$ est une base du $\mathbf{F}_q(X)$-espace vectoriel de dimension 1 $\mathrm{Der}(\mathbf{F}_q(X))$.