DM n° 17 : Polynômes, espaces vectoriels

Correction du problème 1 – La quadrature du cercle

Partie I – Extensions algébriques

1. **Degré d'une extension**

(a) • L'addition correspond à l'addition du corps L. Par définition, $(L,+)$ est un groupe abélien.
• La multiplication par un scalaire de K est la restriction à K (pour la variable scalaire). La multiplication de L étant associative, et distributive sur l'addition, on en déduit toutes les propriétés requises pour un espace vectoriel.

Ainsi, $\boxed{L \text{ est un } K\text{-espace vectoriel}}$.

(b) Soit $(a_1,\dots,a_n)$ une base de L sur K, et $(b_1,\dots,b_m)$ une base de M sur L. En particulier, $n=\dim_K(L)$ et $m=\dim_L(K)$.

Montrons que $(a_ib_j)_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}$ est une base de M sur K.

• Soit $(\lambda_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}$ une famille de scalaires de K tels que

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\lambda_{i,j}a_ib_j=0.$$

On a alors :

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{n}\lambda_{i,j}a_i\right)b_j.$$

Or, les a_i sont dans L, donc les sommes $\sum_{i=1}^{n}\lambda_{i,j}a_i$ sont des éléments de L. Par liberté sur L de la famille $(b_i)_{i\in[\![1,m]\!]}$, on en déduit que pour tout $j\in[\![1,m]\!]$, on a :

$$\sum_{i=1}^{n}\lambda_{i,j}a_i=0.$$

La liberté de la famille (a_i) sur K nous permet alors de conclure que pour tout $(i,j)\in[\![1,n]\!]\times[\![1,m]\!]$, $\lambda_{i,j}=0$.

Ainsi, $(a_ib_j)_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}$ est libre sur K.

• Soit $x\in M$. Comme (b_i) est génératrice sur L, il existe des éléments $\mu_1,\dots,\mu_m$ de L tels que

$$x=\sum_{j=1}^{m}\mu_jb_j.$$

Or, les μ_j étant dans L, et (a_i) étant une famille génératrice de L sur K, pour tout $j\in[\![1,m]\!]$, il existe une famille $(\lambda_{i,j})_{i\in[\![1,n]\!]}$, telle que

$$\mu_j=\sum_{i=1}^{n}\lambda_{i,j}a_i.$$

On a alors :

$$x=\sum_{j=1}^{m}\sum_{i=1}^{n}\lambda_{i,j}a_ib_j.$$

Ainsi, la famille $(a_ib_j)_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}$ est génératrice de M sur K.

on en déduit que $(a_i b_j)_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}$ est une base de M sur K.

Cette base étant de cardinal fini nm, on en déduit que M est de dimension finie sur K, donc que $\boxed{\text{l'extension } M : K \text{ est de degré fini}}$, et que

$$\dim_K(M) = \dim_K(L)\dim_L(M) \qquad \text{soit:} \qquad \boxed{[M:K] = [M:L][L:K]}.$$

2. **Adjonction d'un élément à un corps**

(a) L'intersection de tous les sous-corps de L contenant K et α est un corps (stabilité par intersection), et contient K et α. C'est aussi clairement le plus petit. D'où l'$\boxed{\text{existence de } K(\alpha)}$.

Par ailleurs, comme dans la première question, $K(\alpha)$ est un espace vectoriel sur K, et est muni d'une structure d'anneau (puisque c'est un corps). L'associativité de la multiplication d'un corps, ainsi que sa commutativité, assure que pour tout $\lambda \in K$, et tout $x, y \in K(\alpha)$, $\lambda(xy) = (\lambda x)y = x(\lambda y)$.

Ainsi, $\boxed{K(\alpha) \text{ est une algèbre sur } K}$.

(b) On suppose dans cette question que α est algébrique.

i. Comme α est algébrique, il existe un polynôme P non nul tel que $P(\alpha) = 0$. L'ensemble des degrés des polynômes non nuls annulant α est donc un sous-ensemble non vide de $\mathbb{N}$, et admet un minimum. Soit Q_α un polynôme réalisant ce minimum, et P_α le polynôme unitaire obtenu en divisant Q_α par son coefficient dominant. Ainsi, $\boxed{P_\alpha \text{ est un polynôme unitaire de degré minimal annulant } \alpha.}$

Supposons P_α non irréductible. Il existe alors deux polynômes non constants Q et R dans $K[X]$ tels que $P_\alpha = QR$. On a alors

$$P_\alpha(\alpha) = Q(\alpha)R(\alpha),$$

et l'intégrité de L amène alors $Q(\alpha) = 0$, ou $R(\alpha) = 0$. Or, comme Q et R sont non constants, ils divisent strictement L. Quitte à les diviser par leur coefficient dominant, on a donc trouvé un polynôme unitaire contredisant la minimalité du degré de P_α.

Ainsi, $\boxed{P_\alpha \text{ est irréductible dans } K[X]}$.

ii. L'application linéaire φ est bien définie par la description de l'énoncé (elle est définie sur une base).

Soit P et Q deux polynômes de $K[X]$. On les décrit par leurs coefficients dans K :

$$P = \sum_{i=0}^{k} a_i X^i \qquad \text{et} \qquad Q = \sum_{i=0}^{\ell} b_i X^i.$$

On a alors, par linéarité de φ :

$$\varphi(PQ) = \varphi\left(\sum_{i=0}^{k}\sum_{j=0}^{\ell} a_i b_j X^{i+j}\right) = \sum_{i=0}^{k}\sum_{j=0}^{\ell} a_i b_j \varphi(X^{i+j}).$$

La définition de φ amène donc :

$$\varphi(PQ) = \sum_{i=0}^{k}\sum_{j=0}^{\ell} a_i b_j \alpha^{i+j} = \left(\sum_{i=0}^{k} a_i\alpha^i\right)\left(\sum_{j=0}^{\ell} b_j\alpha^j\right).$$

On utilise à nouveau la linéarité pour conclure que

$$\varphi(PQ) = \varphi(P)\varphi(Q).$$

Ainsi, $\boxed{\varphi \text{ est un morphisme d'algèbre}}$.

Le noyau de φ est l'ensemble des polynômes annulateurs de α. Les polynômes annulateurs sont les éléments de l'idéal (P_α). En effet si P est un polynôme annulateur de α, alors $P \wedge P_\alpha$ aussi (par une relation de Bézout). Comme P_α est de degré minimal, il en résulte que $P \wedge P_\alpha = P_\alpha$, donc P_α divise P, d'où notre assertion.

Ainsi, $\mathrm{Ker}(\varphi) = (P_\alpha)$.

iii. L'application φ définit, par passage au quotient, un morphisme d'anneaux injectif

$$\tilde{\varphi} : K[X]/(\mathrm{Ker}(\varphi)) \longrightarrow K(\alpha).$$

Par ailleurs, étant donné $\overline{P}$ dans $K[X]/(\mathrm{Ker}(\varphi))$ représenté par P, si $\overline{P} \neq 0$, alors $P \wedge P_\alpha \neq P_\alpha$, et $P \wedge P_\alpha$ divise P_α. Par irréductibilité de P_α, on a $P \wedge P_\alpha = 1$, donc P et P_α sont premiers entre eux. Une relatin de Bézout amène alors l'existence de U et V tels que $UP + VP_\alpha = 1$. En réduisant dans le quotient, il vient donc $\overline{UP} = 1$, et par commutativité, on en déduit que $\overline{P}$ est inversible.

Par conséquent, $K[X]/(\mathrm{Ker}(\varphi)) = K[X]/(P_\alpha)$ est un corps. Son image par le morphisme $\tilde{\varphi}$ est donc un sous-corps de $K(\alpha)$. Ce sous-corps contient K et α (image de $\overline{X}$). Donc par minimalité de $K(\alpha)$, on a

$$\mathrm{Im}(\tilde{\varphi}) = K(\alpha).$$

Ainsi, $\tilde{\varphi}$ est surjective.

On en déduit que $\tilde{\varphi}$ est un isomorphisme d'anneaux (donc aussi de corps).

Ainsi, $\boxed{K[X]/(P_\alpha) \text{ est isomorphe à } K(\alpha) \text{ en tant que corps}}$.

iv. La projection canonique p est clairement K-linéaire.

- La famille $(p(1), \cdots, p(X^{d-1})) = (1, \alpha, \cdots \alpha^{p-1})$ est libre dans le K-espace vectoriel $K[X]/(P_a)$, sinon on en déduirait l'existence d'un polynôme Q de $K[X]$ non nul de degré strictement plus petit que d tel que $p(Q) = 0$, c'est-à-dire $Q \in (P_a)$, ou encore, $P_a \mid Q$. Ceci est impossible.
- La famille $(p(1), \cdots, p(X^{d-1}))$ est génératrice de $K[X]/(P_a)$, car étant donné un élément $\tilde{P}$ de P_a, représenté par un polynôme P (c'est-à-dire $p(P) = \tilde{P}$), le reste R de la division de P par P_a vérifie $p(R) = P(P) = \tilde{P}$. Ainsi, tout élément de $K[X]/(P_a)$ est représenté par un polyôme de degré au plus $d - 1$. Notons
$$R = \sum_{k=0}^{d-1} a_k X^k.$$
On a alors
$$\tilde{P} = \sum_{k=0}^{d-1} a_k p(X^k) \in \mathrm{Vect}(p(1), \dots, p(X^{d-1})).$$

Ainsi, $\boxed{(p(1), \cdots, p(X^{d-1})) \text{ est une base de } K[X]/(P_\alpha)}$.

3. **Caractérisation des éléments algébriques**
   - Supposons que α est algébrique, et notons comme plus haut P_α un polynôme unitaire minimal.
     On vérifie assez facilement que le morphisme de corps $\tilde{\varphi}$ introduit précédemment respecte aussi la structure de K-espace vectoriel. Pour le montrer, il suffit de vérifier la compatibilité avec le produit par un scalaire (les autres propriétés étant incluse dans la propriété de morphisme de corps). Cela provient de la linéarité initiale de φ (avant quotient) :
     $$\tilde{\varphi}(\lambda\overline{P}) = \tilde{\varphi}((\overline{\lambda P}) = \varphi(\lambda P) = \lambda\varphi(P) = \lambda\tilde{\varphi}(P).$$
     Ainsi, $\tilde{\varphi}$ est un isomorphisme de K-espaces vectoriels. Comme $K[X]/(P_\alpha)$ est de dimension finie (on en a trouvé une base de cardinal fini d), il en est donc de même de $K(\alpha)$, qui a même dimension. On peut même affirmer que le degré de l'extension $K(\alpha) : K$ est égal au degré du polynôme minimal de α.
   - Réciproquement, si $[K(\alpha) : K] < +\infty$, alors $K(\alpha)$ ne contient pas de famille libre infinie, donc la famille $(\alpha^n)_{n\in\mathbb{N}}$ est liée sur K. Une relation non trivial donne un polynôme annulateur de α à coefficients dans K, permettant d'affirmer que α est algébrique sur K.

   Ainsi, $\boxed{\alpha \text{ est algébrique sur } K \text{ si et seulement si } [K(\alpha) : K] < +\infty}$.
4. **Produit d'éléments algébriques**.
   (a) Si $[L : K]$ est fini, alors pour tout $\alpha \in L$, puisque $K(\alpha)$ est un sous-K-espace vectoriel de L, lui-même de dimension finie sur K, on en déduit que $K(\alpha)$ est aussi de dimension finie sur K. La question précédente nous permet d'affirmer que α est algébrique sur K.
   Ainsi, ceci étant valable pour tout $\alpha \in L$, $\boxed{L \text{ est algébrique sur } K}$.

(b) Soit $\alpha \in M$. Si α est algébrique sur K, il existe un polynôme $P \in K[X]$ tel que $P(\alpha) = 0$. Or $K \subset L$, donc $K[X] \subset L[X]$. Ainsi, il existe aussi $P \in L[X]$ (le même) tel que $P(\alpha) = 0$. Donc $\boxed{\alpha \text{ est aussi algébrique sur } L}$.

(c) Soit α et β deux élément de L, algébriques sur K. On déduit de la question précédente que β est aussi algébrique sur $K(\alpha)$. On a alors, d'après la question 3, $[K(\alpha) : K] < +\infty$ et $[K(\alpha)(\beta) : K(\alpha)] < +\infty$. La question 1(b) montre alors que $[K(\alpha)(\beta) : K] < +\infty$, et la question 4(a) permet de conclure que $\boxed{\text{l'extension } K(\alpha)(\beta) \text{ est algébrique sur } K}$.

(d) Or, α et β sont éléments du corps $K(\alpha)(\beta)$, donc aussi $\alpha\beta$. Ainsi, d'après la question 4(c), $\boxed{\alpha\beta \text{ est algébrique}}$.

Partie II – Transcendance de π

1. On suppose que π est algébrique (sur $\mathbb{Q}$). De plus, i est aussi algébrique, puisque racine du polynôme $X^2 + 1$ à coefficients rationnels. Ainsi, sous l'hypothèse que π est algébrique, et d'après la question I-4(d), on peut conclure que $\boxed{\mathrm{i}\,\pi \text{ est aussi algébrique}}$.

2. Soit P un polynôme minimal unitaire annulant $\mathrm{i}\,\pi$, et soit n son degré.

(a) Le calcul d'un PPCM de P et Q se fait par l'algorithme d'Euclide étendu. Les restes successifs dans cet algorithme seront les mêmes qu'on fasse l'algorithme dans $K[X]$ ou dans $L[X]$. Ainsi, le PPCM (unitaire) est invariant par extension de corps.

Par conséquent, puisque dire que Q et R sont premiers entre eux équivaut à dire que 1 est le PPCM unitaire de Q et R, et que le PPCM unitaire est le même dans $K[X]$ et dans $L[X]$, on peut affirmer que $\boxed{Q \text{ et } R \text{ sont premiers entre eux dans } K[X] \text{ si et seulement s'ils le sont dans } L[X].}$

(b)
- $\boxed{P \text{ est irréductible}}$ dans $\mathbb{Q}[X]$ d'après la question I-2(b)-i.
- Si P admet une racine multiple dans $\mathbb{C}$, P et P' ne sont pas premiers entre eux dans $\mathbb{C}[X]$ (ils ont une racine commune), donc pas non plus dans $\mathbb{Q}[X]$ d'après la question précédente. Ainsi, $P' \wedge P$ est un diviseur non constant de P. Comme P est irréductible, on en déduit que $P' \wedge P = P$ (les deux étant unitaires), puis $P \mid P'$, ce qui est absurde, P n'étant pas constant.
  Donc $\boxed{P \text{ n'admet que des racines simples dans } \mathbb{C}}$.
- Le nombre de racines est au moins égal à 2, car d'après le théorème de d'Alembert-Gauss, il est égal au degré de P, qui ne peut pas être 1 (cela signifierait que $\mathrm{i}\,\pi \in \mathbb{Q}$, alors que cette quantité n'est même par réelle !) Donc $\boxed{n \geqslant 2}$.

3. (a) Soit σ un élément de $\mathcal{S}_n$. On a alors :

$$Q_0(X, X_{\sigma(1)}, \dots, X_{\sigma(n)}) = \prod_{I \subset [\![1,n]\!]} \left(X - \sum_{i \in I} X_{\sigma(i)} \right) = \prod_{I \subset [\![1,n]\!]} \left(X - \sum_{i \in \sigma(I)} X_{\sigma(i)} \right).$$

Or, σ induit une bijection de $\mathcal{P}([\![1,n]\!])$ lui-même. Ainsi, en posant $J = \sigma(I)$ (donc $I = \sigma^{-1}(J)$), on obtient :

$$Q_0(X, X_{\sigma(1)}, \dots, X_{\sigma(n)}) = \prod_{IJ \subset [\![1,n]\!]} \left(X - \sum_{i \in J} X_{\sigma(i)} \right) = Q_0(X, X_1, \dots, X_n)$$

Ainsi, $\boxed{Q \text{ est symétrique par rapport aux variables } X_1, \dots, X_n}$.

(b) Le polynôme Q_0 s'écrit donc comme polynôme en les fonctions symétriques élémentaires des X_i, à coefficients dans $\mathbb{Z}[X]$. Or, en évaluant les X_i aux γ_i, le polynôme Q_1 s'exprime donc comme combinaison linéaire d'éléments de $\mathbb{Z}[X]$, donc les coefficients sont des produits de fonctions symétriques élmentaires en les α_i. Or, d'après les relations de Viète, ces fonctions symétriques élémentaires en les α_i sont aux signe près, les coefficients du polynôme unitaire P dont les α_i sont les racines. Comme $P \in \mathbb{Q}[X]$, on en déduit que Q_1 est combinaison linaire à coefficients rationnels de polynômes de $\mathbb{Z}[X]$. Ainsi, $\boxed{Q_1 \in \mathbb{Q}[X].}$

(c) Remarquons d'abord que $0 = \prod_{i=1}^{n} (\mathrm{e}^{\alpha_i} + 1)$. En effet, le facteur correspondant à $i = 1$ est $\mathrm{e}^{\mathrm{i}\,\pi} + 1 = 0$.

Le développement du produit amène :

$$\prod_{i=1}^{n} (\mathrm{e}^{\alpha_i} + 1) = \sum_{I \subset [\![1,n]\!]} \prod_{i \in I} e^{\alpha_i} = \sum_{I \subset [\![1,n]\!]} \mathrm{e}^{\sum_{i \in I} \alpha_i}.$$

Or, la définition de Q_2 donne une factorisation de Q_2 en polynômes de degré 1, fournissant les racines de Q_2, qui sont exactement les $\displaystyle\sum_{i\in I}\alpha_i$. Ainsi

$$\boxed{0=\prod_{i=1}^{n}(\mathrm{e}^{\alpha_i}+1)=\mathrm{e}^{\gamma_0}+\cdots+\mathrm{e}^{\gamma_s}.}$$

4. Soit c le coefficient dominant de Q et p un nombre premier. L'entier r est comme ci-dessus. On définit :

$$f(X)=\frac{c^{rp-1}}{(p-1)!}X^{p-1}(Q(X))^p \qquad \text{et} \qquad F(X)=f(X)+f'(X)+\cdots+f^{(rp+p-1)}(X).$$

(a) On a, pour tout $x\in\mathbb{R}$:

$$g'(x)=\mathrm{e}^{\backslash x}(F'(x)-F(x))=\mathrm{e}^{\backslash x}(f^{(rp+p)}(x)-f(x)).$$

Or, le polynôme Q est de degré r, donc f est de degré $rp+p-1$. On en déduit que $f^{(rp+p)}=0$, d'où :

$$\forall x\in\mathbb{R},\ \boxed{g'(x)=-\mathrm{e}^{-x}f(x)}.$$

(b) On a donc, pour $x\in\mathbb{R}$:

$$-x\int_0^1\mathrm{e}^{(1-\lambda)x}f(\lambda x)\mathrm{d}\lambda=-\int_0^x\mathrm{e}^{x-y}f(y)\ \mathrm{d}y=\mathrm{e}^x\int_0^x(-\mathrm{e}^{-y}f(y))\ \mathrm{d}y=\mathrm{e}^x\left[g(x)\right]_0^x$$

Ainsi,

$$\boxed{-x\int_0^1\mathrm{e}^{(1-\lambda)x}f(\lambda x)\mathrm{d}\lambda=\mathrm{e}^x(\mathrm{e}^{-x}F(x)-F(0))=F(x)-\mathrm{e}^xF(0)}.$$

Évaluons ces expressions aux γ_i, $i\in[\![1,r]\!]$, et sommons les expressions obtenues :

$$\sum_{i=1}^{r}F(\gamma_i)-F(0)\sum_{i=1}^{r}\mathrm{e}^{\gamma_i}=-\sum_{i=1}^{r}\gamma_i\int_0^1\mathrm{e}^{(1-\lambda)\gamma_i}f(\lambda\gamma_i)\mathrm{d}\lambda.$$

La question 3(c) amène alors :

$$\boxed{\sum_{j=1}^{r}F(\gamma_j)+mF(0)=-\sum_{j=1}^{r}\gamma_j\int_0^1\mathrm{e}^{(1-\lambda)\gamma_j}f(\lambda\gamma_j)\mathrm{d}\lambda}.$$

(c) Le polynôme f ayant un facteur Q élevé à la puissance p, tout racine γ_j de Q est racine de f de multiplicité p au moins. Ainsi, par caractérisation de la multiplicité, pour tout $k\in[\![1,p-1]\!]$, $\boxed{f^{(k)}(\gamma_j)=0}$.

(d) Notons $g=\frac{(p-1)!}{c^{pr-1}}f$. Ainsi, g est un polynôme à coefficients entiers.

Montrons que pour tout $k\in\mathbb{N}$, il existe des polynômes $A_{k,0},\dots,A_{k,p}$, à coefficients entiers, tels que

$$g^{(k)}=\sum_{\ell=0}^{p}\frac{p!}{(p-\ell)!}Q^{p-\ell}A_{k,\ell},$$

et tel que pour tout ℓ, $\deg Q^{p-\ell}A_{k,\ell}\leqslant pr+p-1$.

Cette propriété est vraie pour $k=0$, en posant $A_{0,0}=X^{p-1}$ et $A_{0,i}=0$ pour $i>0$.

Supposons que la propriété soit vérifiée à un certain rang k, alors

$$g^{(k+1)}=\sum_{\ell=0}^{p-1}\frac{p!}{(p-\ell-1)!}Q^{p-\ell-1}A_{k,\ell}Q'+\sum_{\ell=0}^{p}\frac{p!}{(p-\ell)!}Q^{p-\ell}A'_{k,\ell}.$$

On définit alors $A_{k+1,\ell}=A_{k,\ell-1}Q'+A'_{k,\ell}$ si $\ell\in[\![1,p-1]\!]$, et $A_{k+1,\ell}=A'_{k,\ell}$ si $\ell=0$. Ces polynômes sont bien à coefficients entiers, et donnent la relation voulue au rang $k+1$. On vérifie facilement la condition sur les degrés.

Ainsi, d'après le principe de récurrence, pour tout $k \in \mathbb{N}$, il existe des polynômes $A_{k,0}, \dots, A_{k,p}$, à coefficients entiers, tels que

$$g^{(k)} = \sum_{\ell=0}^{p} \frac{p!}{(p-\ell)!} Q^{p-\ell} A_{k,\ell}.$$

Soit alors $h_k(X) = p! A_{k,p}$. Les γ_i étant racines de Q, on a alors, pour tout $k \in \mathbb{N}$,

$$\sum_{i=1}^{r} g^{(k)}(\gamma_i) = \sum_{i=1}^{r} h_k(\gamma_i).$$

On définit alors

$$H = \frac{1}{p!} \sum_{k=0}^{rp+p-1} h_k = c^{pr-1} \sum_{k=0}^{rp+p-1} A_{k,p}.$$

Ce polynôme H est à coefficients entiers, de degré au plus $pr + p - 1$ (grâce au contrôle des degrés effectué dans la récurrence) et d'après la remarque qui précède, on a :

$$\sum_{i=1}^{r} F(\gamma_i) = pc^{rp-1} \sum_{i=1}^{r} H(\gamma_i).$$

Or, $\sum_{j=1}^{r} H(\gamma_j)$ est alors polynomial en les variables γ_j, à coefficients dans $\mathbb{Z}$, et clairement symétrique. Donc, d'après le résultat admis, il s'exprime comme polynôme à coefficients entiers en les fonctions symétriques des γ_j, donc, d'après les relations de Viète, comme polynôme en les $\frac{c_i}{c}$, à coefficients entiers, où les c_i sont les coefficients entiers de Q.

Par ailleurs, le résultat admis sur les polynômes symétriques stipule que ce polynôme en les $\frac{c_i}{c}$ est de degré au plus égal au degré de H, à savoir au plus $pr + p - 1$. Ainsi, $\sum_{j=1}^{r} H(\gamma_j)$ s'exprime comme combinaison à coefficients entiers d'expressions $\frac{d}{c^k}$, où les d sont entiers et les exposants k sont inférieurs à $pr + p - 1$. Par conséquent, $c^{pr-1} \sum_{j=1}^{r} H(\gamma_j)$ est un entier, que nous notons N.

Nous avons alors

$$\sum_{j=1}^{r} F(\gamma_j) = pN,$$

donc $\boxed{\sum_{j=1}^{r} F(\gamma_j) \text{ est un entier divisible par } p}$.

(e) On a, pour tout $k \in [\![0, rp + p - 1]\!]$, d'après la formule de Leibniz :

$$f^{(k)}(X) = \frac{c^{pr-1}}{(p-1)!} \sum_{i=0}^{\min(k,p-1)} \binom{k}{i} \frac{(p-1)!}{(p-1-i)!} X^{p-1-i} (Q(X)^p)^{(k-i)}.$$

Ainsi :

- si $k < p - 1$, tous les termes de la somme ont un facteur X, donc $f^{(k)}(0) = 0$ (cela se voit aussi en remarquant que 0 est racine de multiplicité $p - 1$ de f)
- si $k = p - 1$, seul un terme n'a pas de facteur X, ainsi :

  $$f^{(p-1)}(0) = c^{pr-1} Q(0)^p = c^{pr-1} c_0^p,$$

  où $c_0 = Q(0)$ est le coefficient constant de Q.
- si $k > p - 1$, on obtient également un unique terme sans facteur X :

  $$f^{(k)}(0) = c^{pr-1} \binom{k}{p-1} A(0),$$

  où A est la dérivée $k - p + 1$-ième du polynôme $Q(X)^p$. Or, l'ordre de cette dérivation est au moins 1, et

  $$(Q(X)^p)' = pQ'(X)Q(X)^{p-1} = pB(X),$$

où B est un polynôme à coefficients entiers. Ainsi,

$$A(0) = pB^{(k-p)}(0),$$

et B étant à coefficients entiers, $B^{(k-p)}(0)$ est un entier. Ainsi, $A(0) \equiv 0$ $[p]$, puis $f^{(k)}(0) \equiv 0$ $[p]$. Nous en déduisons que $F(0) \equiv c^{rp-1}c_0^p$ $[p]$, et la question 3(d) permet de conclure :

$$\boxed{\sum_{j=1}^{r} F(\gamma_j) + mF(0) \equiv mc^{rp-1}c_0^p \; [p]}.$$

(f) Soit p un nombre premier vérifiant $p > \max(m, c, c_0)$. Alors, m, c et c_0, étant non nuls (0 n'est pas racine de Q), et non divisibles par p, sont premiers avec p, donc aussi $mc^{rp-1}c_0^p$. Ainsi, $mc^{rp-1}c_0^p \not\equiv 0$ $[p]$, donc $\sum_{j=1}^{r} F(\gamma_j) + mF(0) \not\equiv 0$ $[p]$. En particulier, pour tout nombre premier p suffisamment grand (plus précisément vérifiant $p > \max(m, c, c_0)$), $\boxed{\sum_{j=1}^{r} F(\gamma_j) + mF(0) \text{ est un entier non nul}}$.

5. On montre que le terme de droite (s'exprimant sous forme intégrale), converge vers 0 lorsque le nombre premier p tend vers $+\infty$. En effet, notons $\delta = \max(|\gamma_i|, i \in [\![1, r]\!])$. La fonction $z \mapsto zQ(z)$ est continue, donc bornée sur le compact $\overline{B}(0, \delta) \subset \mathbb{C}$, et de même pour $z \mapsto Q(z)$. Notons M_1 et M_2 deux réels tels que

$$\forall z \in \overline{B}(0, \delta), \quad |zQ(z)| \leqslant M_1 \qquad \text{et} \qquad |Q(z)| \leqslant M_2.$$

Alors, d'après l'inégalité triangulaire intégrale,

$$\left| \int_0^1 \mathrm{e}^{(1-\lambda)\gamma_j} f(\lambda\gamma_j) \mathrm{d}\lambda \right| \leqslant \int_0^1 \left| \mathrm{e}^{(1-\lambda)\gamma_j} \right| \frac{(|c|^r M_1)^{p-1}}{(p-1)!} M_2 |c|^{r-1} \mathrm{d}\lambda.$$

La fonction continue $\lambda \mapsto \left| \mathrm{e}^{(1-\lambda)\gamma_j} \right|$ peut également être majorée par une constante M_3 sur le compact $[0, 1]$, d'où :

$$\left| \int_0^1 \mathrm{e}^{(1-\lambda)\gamma_j} f(\lambda\gamma_j) \mathrm{d}\lambda \right| \leqslant \frac{(|c|^r M_1)^{p-1}}{(p-1)!} |c|^{r-1} M_2 M_3.$$

La comparaison des croissances des suites géométriques et des factorielles permet de justifier que le majorant obtenu converge vers 0 lorsque p tend vers $+\infty$ en étant premier. Ainsi, en notant p_n le n-ième nombre premier (on a bien $p_n \to +\infty$), et f_{p_n} et F_{p_n} les fonctions associées, on a :

$$\forall i \in [\![1, r]\!], \quad \lim_{n \to +\infty} \int_0^1 \mathrm{e}^{(1-\lambda)\gamma_j} f_{p_n}(\lambda\gamma_j) \mathrm{d}\lambda,$$

puis :

$$\lim_{n \to +\infty} \sum_{j=1}^{r} \gamma_j \int_0^1 \mathrm{e}^{(1-\lambda)\gamma_j} f_{p_n}(\lambda\gamma_j) \mathrm{d}\lambda = 0.$$

On a donc

$$\lim_{n \to +\infty} \sum_{j=1}^{r} F_{p_n}(\gamma_j) + mF_{p_n}(0) = 0.$$

Or, il s'agit d'une suite d'entiers. Sa convergence implique donc qu'elle est stationnaire de valeur 0 à partir d'un certain rang. Ceci contredit le fait que pour tout p assez grand (donc tout $p = p_n$ avec n assez grand), cette expression est non nulle (question 4(f)).

Aboutissant à une contradiction, on peut conclure que l'hypothèse initiale portant sur l'algébricité de π est fausse, et on conclut :

$$\boxed{\pi \textbf{ est transcendant.}}$$