ÉCOLE POLYTECHNIQUE OPTION MP

CONCOURS D'ADMISSION 1998

DEUXIÈME COMPOSITION DE MATHÉMATIQUES

(Durée : 4 heures)

L'utilisation des calculatrices n'est pas autorisée pour cette épreuve.

***

On attachera la plus grande importance à la clarté, à la précision et à la concision de la rédaction.

***

On se propose, dans ce problème, de démontrer quelques propriétés des sous-corps du corps des complexes $\mathbb{C}$. On rappelle que, si K est un sous-corps d'un corps K', ce dernier est, en particulier, un K-espace vectoriel, ce qui donne un sens à la K-dimension de K', notée $\dim_K(K')$.

Si K est un corps, on note $K[X]$ l'anneau des polynômes à coefficients dans K. On dit qu'un polynôme de degré > 0 est *irréductible* s'il ne peut pas s'écrire comme produit de deux polynômes de degrés > 0. Un polynôme est *unitaire* si le coefficient de son terme de plus haut degré est égal à 1.

La question 1 est classique et servira surtout à fixer quelques notations ; la question 2 n'est pas utilisée dans la suite.

Première partie

On désigne par K un sous-corps de $\mathbb{C}$, par α un nombre complexe non nul, par $K[\alpha]$ le sous-K-espace vectoriel de $\mathbb{C}$ engendré par les nombres $\alpha^n, n = 0, 1, 2, ...$, enfin par $I_K(\alpha)$ l'ensemble des polynômes de $K[X]$ annulés par α.

1.a) Montrer que les deux conditions suivantes sont équivalentes :

$$(i) \quad \dim_K(K[\alpha]) < +\infty$$
$$(ii) \quad I_K(\alpha) \neq \{0\}.$$

Si elles sont remplies, on dit que α est *K-algébrique*, ce que l'on suppose dans la suite de cette question.

b) Montrer qu'il existe un unique polynôme unitaire $P \in K[X]$ tel que tout élément de $I_K(\alpha)$ soit un multiple de P, et que P est irréductible.

ÉCOLE POLYTECHNIQUE 1998

2ème composition 2/3

Ce polynôme P sera noté $P_K(\alpha)$ et appelé *polynôme K-minimal* de α.

c) Comparer le degré de $P_K(\alpha)$ et $\dim_K(K[\alpha])$.

d) Montrer que $K[\alpha]$ est un corps.

2. *Applications numériques.* On prend $K = \mathbb{Q}$.

a) Déterminer le polynôme $\mathbb{Q}$-minimal de $\alpha = \sqrt{2}$.

b) Déterminer le polynôme $\mathbb{Q}$-minimal de $\alpha = \sqrt{\dfrac{1+\sqrt{5}}{2}}$.

Deuxième partie

On définit K et α comme dans la première partie. On suppose que α est K-algébrique et on pose $n = \dim_K(K[\alpha])$.

3. Montrer que, si P est un élément irréductible de $K[X]$, ses zéros dans $\mathbb{C}$ sont tous simples.

4.a) On note $\lambda_1, \ldots, \lambda_n$ les zéros de $P_K(\alpha)$ dans $\mathbb{C}$. Montrer que, pour tout $i = 1, \ldots, n$, il existe un unique morphisme de K-algèbres σ_i de $K[\alpha]$ dans $\mathbb{C}$ tel que $\sigma_i(\alpha) = \lambda_i$.

b) Obtient-on de cette façon tous les morphismes de K-algèbres de $K[\alpha]$ dans $\mathbb{C}$?

5. Montrer que si β est un élément de $K[\alpha]$ et si les $\sigma_i(\beta)$ sont deux à deux distincts, alors on a $K[\alpha] = K[\beta]$.

6. Etant donné un élément β de $K[\alpha]$, démontrer l'existence de deux éléments β_1 et β_2 de $K[\alpha]$ vérifiant $K[\beta_1] = K[\beta_2] = K[\alpha]$ et $\beta_1 + \beta_2 = \beta$.

[On pourra introduire, pour $i \neq j$, l'ensemble $E_{i,j}$ des éléments λ de K vérifiant

$$\sigma_i(\alpha + \lambda\beta) = \sigma_j(\alpha + \lambda\beta)]$$

QC : * Polynôme caractéristique d'une matrice compagnon
* Théorème de Cayley – Hamilton.

Troisième partie

On fixe un nombre complexe $\mathbb{Q}$-algébrique non nul θ, et on pose $K = \mathbb{Q}[\theta]$, $n = \dim_{\mathbb{Q}}(K)$. On note σ_i, $i = 1, \ldots, n$, les morphismes de $\mathbb{Q}$-algèbres de K dans $\mathbb{C}$.

Dans ce qui suit, α désigne un élément de K ; on appelle M_α l'endomorphisme du $\mathbb{Q}$-espace vectoriel K défini par $M_\alpha(\beta) = \alpha\beta$ pour tout $\beta \in K$, et Δ_α son polynôme caractéristique défini par $\lambda \mapsto$ dét $(\lambda \mathrm{I} - M_\alpha)$.

7. On pose $m = \dim_{\mathbb{Q}}(\mathbb{Q}[\alpha])$, $d = \dim_{\mathbb{Q}[\alpha]}(K)$. Vérifier que, si $(e_1, ..., e_d)$ est une $\mathbb{Q}[\alpha]$ - base de K, les éléments $\alpha^p e_r$ où $p = 0, ..., m-1$ et $r = 1, ..., d$, forment une $\mathbb{Q}$-base de K.

8.a) Démontrer l'égalité $\Delta_\alpha = (P_{\mathbb{Q}}(\alpha))^d$.

[On pourra examiner d'abord le cas où $\mathbb{Q}[\alpha] = K$]

b) Démontrer l'égalité $\mathrm{Tr}(M_\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$.

9. Pour tout n-uple $(\alpha_1, ..., \alpha_n)$ de K^n, on pose

$$D(\alpha_1, ..., \alpha_n) = \text{dét}\left(\mathrm{Tr}(M_{\alpha_i \alpha_j})\right)_{i,j=1,...,n}.$$

Exprimer $D(\alpha_1, ..., \alpha_n)$ en fonction de dét $\left(\sigma_i(\alpha_j)\right)_{i,j=1,...,n}$.

10. Soit $A = \left(A_{i,j}\right)_{i,j=1,...,n}$ une matrice à coefficients dans $\mathbb{Q}$, et soit $\beta_i = \sum_{p=1}^{n} A_{i,p}\alpha_p$. Vérifier que

$$D(\beta_1, ..., \beta_n) = (\text{dét } A)^2 D(\alpha_1, ..., \alpha_n).$$

11. Montrer que

$$D(1, \theta, ..., \theta^{n-1}) = (-1)^{n(n-1)/2} \prod_{i \neq j} (\sigma_i(\theta) - \sigma_j(\theta)).$$

12. Donner une condition nécessaire et suffisante, portant sur $D(\alpha_1, ..., \alpha_n)$, pour qu'un n-uple $(\alpha_1, ..., \alpha_n)$ soit une $\mathbb{Q}$-base de K.

13.a) Vérifier que le polynôme $X^3 - X - 1$ admet un unique zéro réel, que l'on note θ.

b) Déterminer le polynôme $\mathbb{Q}$-minimal de θ.

c) Calculer $D(1, \theta, \theta^2)$.

* *
*

CONCOURS d'ADMISSION à l'ÉCOLE POLYTECHNIQUE 1998
deuxième composition de mathématiques)

Première Partie

N.B. La première question est essentiellement une question de cours. Cependant il a semblé préférable d'en donner une justification directe complète.

I-1.a *(i ⇒ ii)* : si $n = \dim_K(K[\alpha])$ la famille $(1, \alpha, \alpha^2, \ldots, \alpha^n)$ est liée, donc il existe une famille de coefficients $(a_i)_{0\leq i\leq n}$ non nulle telle que $\sum_{i=0}^{n} a_i\alpha^i = 0$; c'est à dire que le polynôme $P = \sum_{i=0}^{n} a_iX^i$ vérifie $P \neq 0$ et $P(\alpha) = 0$ donc $P \in I_K(\alpha) \setminus \{0\}$ d'où *(ii)*.

(ii ⇒ i) : soit P un polynôme non nul appartenant à $I_K(\alpha)$; quitte à multiplier par une constante on peut supposer P unitaire ; soit n son degré : $P = X^n - \sum_{i=0}^{n-1} a_iX^i$. On a donc $\alpha^n = \sum_{i=0}^{n-1} a_i\alpha^i$.

Soit E le K-sous-espace vectoriel de $\mathbf{C}$ engendré par $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$: il est clair, compte tenu de la formule précédente que E est stable par $z \mapsto \alpha z$ et par suite contient tous les α^j pour $j \in \mathbf{N}$. Il en résulte que $E \supset K[\alpha]$ (et par suite $E = K[\alpha]$) donc $\dim_K(K[\alpha]) \leq \dim_K(E) \leq n$, d'où (i).

I-1.b $I_K(\alpha)$ est un idéal de $K[X]$: on sait que tout idéal de $K[X]$ est principal. Rappelons l'argument : soit P un polynôme non nul de degré minimum de $I_K(\alpha)$ que l'on peut prendre unitaire. Pour un polynôme S quelconque de $I_K(\alpha)$ on peut considérer la division euclidienne de S par P : $S = PQ + R$ avec $\deg R < \deg P$. Comme $R = S - PQ \in I_K(\alpha)$ (on vérifie d'ailleurs immédiatement $R(\alpha) = 0$), l'hypothèse $R \neq 0$ contredit le choix de P ; par suite $R = 0$ et $S = PQ$: tout élément de $I_K(\alpha)$ est multiple de P.

Si P_1 unitaire possède la même propriété on a simultanément P divise P_1 et P_1 divise P donc $P_1 = \lambda P$ avec $\lambda \in K$: comme P et P_1 sont unitaires on à $\lambda = 1$ et $P_1 = P$. Ce qui prouve que P est l'unique *générateur* unitaire de $I_K(\alpha)$.

I-1.c Le polynôme $P_K(\alpha)$ est aussi, d'après la construction faite en **b**, le polynôme noté P en **a** *(ii⇒ i)*. On a donc $\dim_K(K[\alpha]) \leq \deg P$; d'après **a** *(i⇒ ii)* on a aussi $\deg P \leq \dim_K(K[\alpha])$.
Finalement $\deg P_K(\alpha) = \dim_K(K[\alpha])$.

I-1.d Soit $a \in K[\alpha] \setminus \{0\}$; l'application de $K[\alpha]$ dans lui-même : $x \mapsto ax$ est K-linéaire et injective (car $x \neq 0$) donc bijective (car l'espace est de dimension finie). Par suite il existe $b \in K[\alpha]$ tel que $ab = 1$ c'est à dire que tout élément non nul de $K[\alpha]$ est inversible. Par suite $K[\alpha]$ est un corps (rappelons que $K[\alpha]$ est commutatif).

I-2.a $\alpha = \sqrt{2}$ est racine de $X^2 - 2$; pour justifier que $X^2 - 2$ est bien le polynôme $\mathbf{Q}$-minimal de $\sqrt{2}$ il suffit de vérifier que $\sqrt{2}$ n'est racine d'aucun polynôme non nul de degré inférieur ou égal à 1 de $\mathbf{Q}[X]$, c'est à dire que $\sqrt{2}$ n'est pas dans $\mathbf{Q}$. Raisonnons par l'absurde : si $\sqrt{2} = \frac{p}{q}$ avec $p, q \in \mathbf{Z} \setminus \{0\}$ premiers entre eux on a $p^2 = 2q^2$ donc 2 divise p , soit $p = 2p'$; il vient $2p'^2 = q^2$ donc 2 divise q ; 2 est diviseur commun à p et q ce qui contredit l'hypothèse p, q premiers entre eux. Par conséquent $\sqrt{2}$ n'est pas rationnel et $X^2 - 2$ est le polynôme $\mathbf{Q}$-minimal de $\sqrt{2}$.

I-2.b Soit $\alpha = \sqrt{\frac{1+\sqrt{5}}{2}}$; on a $\alpha^2 = \frac{1+\sqrt{5}}{2}$ d'où $(2\alpha^2 - 1)^2 = 5$, ou encore $\alpha^4 - \alpha^2 - 1 = 0$. Donc α est racine du polynôme $P = X^4 - X^2 - 1$: pour montrer que ce polynôme est le polynôme $\mathbf{Q}$-minimal de α il suffit de montrer que P est irréductible sur $\mathbf{Q}$ (car le polynôme $\mathbf{Q}$ minimal en étant un diviseur non constant et unitaire ne pourra alors que lui être égal).
Pour montrer que P n'a pas de diviseur dans $\mathbf{Q}[X]$ de degré 1 il suffit de vérifier que P n'a pas de racine rationnelle. Sinon soit $\frac{p}{q} \neq 0$ (P n'admet pas 0 pour racine) une telle racine ($p \in \mathbf{Z}$ et $q \in \mathbf{N} \setminus \{0\}$ avec p, q premiers entre eux). On a alors $p^4 - p^2q^2 - q^4 = 0$ donc $p^4 = (p^2 + q^2)q^2$ d'ou résulte que q divise

p^4 ; or q est aussi premier avec p^4 (corollaire du théorème de Gauss), donc $q = 1$. Alors $p^4 - p^2 - 1 = 0$ entraine que p divise 1 donc $p = \pm 1$. On constate immédiatement que 1 et -1 ne sont pas racines de P donc P n'a pas de diviseur de degré 1 et par suite n'a pas non plus de diviseur de degré 3.
Montrons maintenant que P n'a pas de diviseur de degré 2 dans $\mathbf{Q}[X]$. Sinon P est produit de deux polynômes de degré 2 et on peut supposer le second unitaire :

$$X^4 - X^2 - 1 = P = (aX^2 + bX + c)(X^2 + b'X + c').$$

L'identification donne $a = 1$, $ab' + b = 0$, $ac' + bb' + c = -1$, $bc' + cb' = 0$, $cc' = -1$. On a donc $b' = -b$; si $b \neq 0$ il vient $c' = c$ et $c^2 = -1$ ce qui est impossible. Par suite $b = b' = 0$, $c' = -c - 1$ et $c^2 + c - 1 = 0$. On vérifie encore que cette dernière équation n'a pas de racine dans $\mathbf{Q}$: si $\frac{p}{q}$ irréductible est racine, $p^2 + pq - q^2 = 0$ donc q divise p^2 et par ailleurs premier à p^2 , d'où $q = 1$; puis $p^2 + p - 1 = 0$ donc p divise 1 et $p = \pm 1$; comme 1 et -1 ne sont pas racine de $X^2 + X - 1$ on a la contradiction cherchée. P n'a pas de diviseur de degré 2.

Ainsi $P = X^4 - X^2 - 1$ est irréductible et c'est le polynôme $\mathbf{Q}$-minimal de $\sqrt{\frac{1+\sqrt{5}}{2}}$.

Deuxième Partie

II-3 Soit P irréductible dans $K[X]$; notons Δ le *pgcd* de P et P'. Δ est donc un diviseur de P de degré strictement inférieur à celui de P, par suite $\Delta = 1$. Ainsi P' est premier à P et les zéros de P sont simples.

II-4.a Par définition tout élément de $K[\alpha]$ peut s'écrire $Q(\alpha)$ avec $Q \in K[X]$.
Si σ est un K-morphisme d'algèbre de $K[\alpha]$ dans $\mathbf{C}$ tel que $\sigma(\alpha) = \lambda$ on a $\sigma(\alpha^j) = \lambda^j$ et nécessairement $\sigma(Q(\alpha)) = Q(\lambda)$.

Soit λ une des racines de $P_K(\alpha)$; définissons donc σ de $K[\alpha]$ dans $\mathbf{C}$ par $\sigma(Q(\alpha)) = Q(\lambda)$. Pour légitimer cette définition il faut constater que si $x = Q_1(\alpha) = Q_2(\alpha) \in K[\alpha]$ alors les images de x calculées à partir de Q_1 et Q_2 coïncident : $Q_1(\lambda) = Q_2(\lambda)$. Or comme $(Q_1 - Q_2)(\alpha) = 0$, $P_K(\alpha)$ divise $Q_1 - Q_2$; par suite, puisque λ est racine de $P_K(\alpha)$ on a $(Q_1 - Q_2)(\lambda) = 0$ et $Q_1(\lambda) = Q_2(\lambda)$. Donc σ est bien défini.
Il est alors immédiat de vérifier que σ est un morphisme de K-algèbre. Notant $Q, Q_1, Q_2 \in K[X]$ et $t \in K$:
$\sigma(Q_1(\alpha) + \mathbf{Q}_2(\alpha)) = \sigma((Q_1 + Q_2)(\alpha)) = (Q_1 + Q_2)(\lambda) = Q_1(\lambda) + Q_2(\lambda) = \sigma(Q_1(\alpha)) + \sigma(\mathbf{Q}_2(\alpha))$
$\sigma(tQ(\alpha)) = \sigma((tQ)(\alpha)) = (tQ)(\lambda) = tQ(\lambda) = t\sigma(Q(\alpha))$
$\sigma(Q_1(\alpha)\mathbf{Q}_2(\alpha)) = \sigma((Q_1Q_2)(\alpha)) = (Q_1Q_2)(\lambda) = Q_1(\lambda)Q_2(\lambda) = \sigma(Q_1(\alpha))\sigma(\mathbf{Q}_2(\alpha))$
$\sigma(1) = 1$ (utiliser $Q = 1$).
Il y a donc un unique morphisme de $K[\lambda]$ dans $\mathbf{C}$ dont l'image de α est λ. Il suffit d'appliquer ce résultat à $\lambda_1, \lambda_1, \ldots, \lambda_n$.

II-4.b On obtient ainsi tous les morphismes de K-algèbre de $K[\alpha]$ dans $\mathbf{C}$: si σ est un tel morphisme on a pour tout $Q \in K[X]$, $\sigma(Q(\alpha)) = Q(\sigma(\alpha))$ donc en particulier, avec $Q = P_K(\alpha)$: $(P_K(\alpha))(\lambda) = \sigma((P_K(\alpha))(\alpha)) = \sigma(0) = 0$. Donc λ est une des racines de $P_K(\alpha)$: σ est donc un des morphismes construits précédemment.

II-5 Pour $\beta \in K[\alpha]$ notons $K' = K[\beta]$; comme $K[\beta] \subset K[\alpha]$ on a $\dim_K(K[\beta])$ fini et d'après **I-1.d** K' est un corps.
On a évidemment $K[\alpha] = K'[\alpha]$ (puisque $K \subset K' \subset K[\alpha]$). D'après la question précédente il y a exactement $\dim_{K'} K[\alpha]$ morphismes de K'-algèbre de $K[\alpha]$ dans $\mathbf{C}$. Un tel morphisme est d'une part dans la liste des K-morphismes d'algèbre de $K[\alpha]$ dans $\mathbf{C}$, et d'autre part laisse fixe tout élément de K' (puisqu'il laisse fixe 1). Par hypothèse les $\sigma_i(\beta)$ sont tous distincts, donc en notant j l'injection canonique de $K[\alpha]$ dans $\mathbf{C}$, on a pour $\sigma_i \neq j$: $\sigma_i(\beta) \neq \beta$ et σ_i n'est pas un K'-morphisme de $K[\alpha]$ dans $\mathbf{C}$. Par suite il n'existe qu'un seule morphisme de K' algèbre de $K[\alpha]$ dans $\mathbf{C}$, c'est l'injection canonique j. Il en résulte que $\dim'_K(K[\alpha]) = 1$ et donc $K' = K[\alpha]$ (K'-espaces vectoriels emboités de même dimension).
On a ainsi prouvé que $K[\beta] = K' = K[\alpha]$.

II-6 λ étant un élément de K à choisir, posons $\beta_1 = \alpha + \lambda\beta$ et $\beta_2 = -\alpha + (1 - \lambda)\beta$. On a $\beta_1 + \beta_2 = \beta$.

Pour montrer que $K[\beta_1] = K[\alpha]$ et $K[\beta_2] = K[\alpha]$ il suffit de prouver, d'après la question précédente, que d'une part les $\sigma_i(\beta_1)$, d'autre part les $\sigma_i(\beta_2)$ sont distincts. Il faut donc prendre λ de façon que pour $i \neq j$ on ait

$$\sigma_i(\alpha + \lambda\beta) \neq \sigma_j(\alpha + \lambda\beta) \qquad \text{et} \qquad \sigma_i(-\alpha + (1-\lambda)\beta) \neq \sigma_j(-\alpha + (1-\lambda)\beta)$$

Or chacune des équations en λ : $\sigma_i(\alpha+\lambda\beta) = \sigma_j(\alpha+\lambda\beta)$ admet au plus une racine (car elle est linéaire et non vérifiée pour $\lambda = 0$).
Il en est de même pour : $\sigma_i(-\alpha + (1-\lambda)\beta) = \sigma_j(-\alpha + (1-\lambda)\beta)$ (linéaire non vérifiée pour $\lambda = 1$).
Il n'y a donc qu'un nombre fini de valeurs à éviter pour le choix de λ, et comme K (contenant $\mathbf{Q}$) est infini le choix de λ comme annoncé est possible.
Par suite il existe β_1 et β_2 dans $K[\alpha]$ tels que $\beta = \beta_1 + \beta_2$ et $K[\beta_1] = K[\beta_2] = K[\alpha]$.

Troisième Partie

III-7 Remarquons au préalable qu'il résulte de la question **1.c** appliquée à $K = \mathbf{Q}$ que $(1, \alpha, \alpha^2, \ldots, \alpha^{m-1})$ est une $\mathbf{Q}$-base de $\mathbf{Q}[\alpha]$ (famille libre et de cardinal égal à la dimension de l'espace).
Pour $x \in K$ il existe des $x_i \in \mathbf{Q}[\alpha]$ tels que $x = \sum_{i=1}^{d} x_i e_i$; pour chaque $x_i \in \mathbf{Q}[\alpha]$ il existe des coefficients $t_{i,j} \in \mathbf{Q}$ tels que $x_i = \sum_{j=0}^{m-1} t_{i,j}\alpha^j$. Par suite $x = \sum_{i=1}^{d}\sum_{j=0}^{m-1} t_{i,j}\alpha^j e_i$: donc $(\alpha^p e_r)_{(p,r)\in\{0,\ldots,m-1\}\times\{1,\ldots,d\}}$ est une famille génératrice.
Montrons que cette famille est libre : si $\sum_{i=1}^{d}\sum_{j=0}^{m-1} t_{i,j}\alpha^j e_i = 0$ on a $\sum_{i=1}^{d}(\sum_{j=0}^{m-1} t_{i,j}\alpha^j)e_i = 0$ donc puisque $\sum_{j=0}^{m-1} t_{i,j}\alpha^j \in \mathbf{Q}[\alpha]$ et $(e_i)_{i\in\{1,\ldots,d\}}$ libre, $\sum_{j=0}^{m-1} t_{i,j}\alpha^j = 0$; comme $(\alpha^j)_{j\in\{0,\ldots,m-1\}}$ est libre il en résulte enfin $t_{i,j} = 0$. Ainsi $(\alpha^p e_r)_{(p,r)\in\{0,\ldots,m-1\}\times\{1,\ldots,d\}}$ est libre. Nous avons donc prouvé que c'est une base.

III-8.a On vérifie immédiatement que $M_\alpha^j(\beta) = \alpha^j\beta$. Il en résulte que pour tout polynôme $R \in \mathbf{Q}[X]$ on a $R(M_\alpha) = M_{R(\alpha)}$. D'après le théorème d'Hamilton-Cayley $\Delta_\alpha(M_\alpha) = 0$ donc $M_{\Delta_\alpha(\alpha)} = 0$ et par suite $\Delta_\alpha(\alpha) = 0$. Donc $P_{\mathbf{Q}}(\alpha)$ divise Δ_α.
Dans le cas $K = \mathbf{Q}[\alpha]$, Δ_α est unitaire de degré m donc $\Delta_\alpha = P_{\mathbf{Q}}(\alpha)$.
Ce raisonnement permet d'éviter tout calcul mais l'expression de M_α dans la base $(1, \alpha, \ldots, \alpha^{m-1})$ conduit à une matrice compagnon dont le calcul du déterminant est immédiat.
Si $\alpha^m = \sum_{i=0}^{m-1} a_i\alpha^i$ on a $P_{\mathbf{Q}}(\alpha) = X^m - \sum_{i=0}^{m-1} a_i\alpha^i$ et la matrice de M_α (dans le cas $K = \mathbf{Q}[\alpha]$) est $\begin{pmatrix} 0 & 0 & 0 & \ldots & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & a_{m-1} \end{pmatrix}$ de polynôme minimal et de polynôme caractéristique $P_{\mathbf{Q}}(\alpha)$.
Considérons maintenant le cas général : chaque $E_i = \text{vect}(e_i, \alpha e_i, \alpha^2 e_i, \ldots, \alpha^{m-1}e_i) = \mathbf{Q}[\alpha]e_i$ est un $\mathbf{Q}$-sous-espace vectoriel de K stable par M_α et la matrice de l'endomorphisme induit par M_α sur ce sous-espace, dans la base $(e_i, \alpha e_i, \ldots, \alpha^{m-1}e_i)$ est la matrice A. K étant la somme directe des espaces E_i le polynôme caractéristique de M_α est le produit des d polynômes caractéristiques des induits, tous égaux à $P_{\mathbf{Q}}(\alpha)$ (polynôme caractéristique de A). Donc $\Delta_\alpha = (P_{\mathbf{Q}}(\alpha))^d$.
Remarque : on peut aussi dire que la matrice de M_α dans la base considérée de K est diagonale en d blocs A.

III-8.b La trace de M_α est la somme des racines de Δ_α c'est à dire d fois la somme des racines de $P_{\mathbf{Q}}(\alpha)$. Pour prouver l'égalité $\text{Tr}(M_\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$ il suffit de montrer que la liste $(\sigma_i(\alpha))_{1\leq i\leq n}$ contient exactement d fois chaque racine de $P\mathbf{Q}(\alpha)$.
Remarquons d'abord que $(P_{\mathbf{Q}}(\alpha))(\alpha) = 0$ entraine pour tout i $(P_{\mathbf{Q}}(\alpha))(\sigma_i(\alpha)) = \sigma_i((P_{\mathbf{Q}}(\alpha))(\alpha)) = 0$ car les coefficients de $P_{\mathbf{Q}}(\alpha)$ sont dans $\mathbf{Q}$ donc fixes par σ_i. Ainsi tous les $\sigma_i(\alpha)$ sont racines de $P_{\mathbf{Q}}(\alpha)$.
Fixons maintenant un indice k et montrons qu'il y a exactement d indices j tels que $\sigma_j(\alpha) = \sigma_k(\alpha)$.
Il est commode ici de considérer σ_i comme un isomorphisme sur son image (σ_i est injectif car c'est un

morphisme de corps : on le corestreint à son image). Alors $\sigma_j\sigma_k^{-1}$ est un isomorphisme de $K' = \sigma_k(K)$ sur un sous-corps de $\mathbf{C}$ et $\sigma_j(\alpha) = \sigma_k(\alpha) = \alpha'$ équivaut à $\sigma_j\sigma_k^{-1}(\alpha') = \alpha'$; ce qui équivaut encore à : $\sigma_j\sigma_k^{-1}$ est isomorphisme de K' sur un sous-corps de $\mathbf{C}$ qui laisse fixe α' et donc $\mathbf{Q}[\alpha']$. Inversement si μ est un $\mathbf{Q}[\alpha']$-isomorphisme de K' sur un sous corps de $\mathbf{C}$ alors $\tau = \mu\sigma_k$ est un isomorphisme de K sur un sous-corps de $\mathbf{C}$ tel que $\tau(\alpha) = \alpha' = \sigma_k(\alpha)$: c'est donc un des σ_j recherché (le caractère morphisme de $\mathbf{Q}$-algèbre est alors automatique). L'application $\mu \mapsto \mu\sigma_k$ étant bijective de l'ensemble des isomorphismes de K' sur des sous-corps de $\mathbf{C}$ laissant fixe α' vers l'ensemble des σ_j cherché, il suffit de rechercher le nombre de ces isomorphismes. Un tel isomorphisme laisse automatiquement fixe tous les éléments de $\mathbf{Q}[\alpha']$ et c'est donc un isomorphisme de $\mathbf{Q}[\alpha']$-algèbre. Leur nombre est donc $\dim_{\mathbf{Q}[\alpha']} K'$ (application de la question **4** avec changement de notations et les conventions faites). Comme σ_k est un isomorphisme de K sur K' qui envoie $\mathbf{Q}[\alpha]$ sur $\mathbf{Q}[\alpha']$ les familles $\mathbf{Q}[\alpha']$-libre de K' correspondent par σ_k aux familles $\mathbf{Q}[\alpha]$-libre de K : par suite $\dim_{\mathbf{Q}[\alpha']} K' = \dim_{\mathbf{Q}[\alpha]} K = d$.
Nous avons ainsi prouvé que si une racine de $P_{\mathbf{Q}}(\alpha)$ figure dans la liste des $\sigma_i(\alpha)$ elle y figure d fois. Il y a donc $n/d = m$ $\sigma_i(\alpha)$ distincts, c'est à dire que toutes les racines de $P_{\mathbf{Q}}(\alpha)$ sont dans la liste des $\sigma_i(\alpha)$ (facile à voir aussi directement à l'aide de la deuxième partie). Ce qui achève la démonstration du résultat annoncé et prouve l'égalité proposée.

III-9 Il en résulte $\mathrm{Tr}(M_{\alpha_i\alpha_j}) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)$ La matrice $\big(\mathrm{Tr}M_{\alpha_i\alpha_j}\big)$ est donc le produit de la matrice $B = \big(\sigma_j(\alpha_i)\big)$ par sa transposée. Le déterminant est donc $\det(B)^2$.
On a $\quad D(\alpha_1, \ldots, \alpha_n) = \Big(\det\big(\sigma_i(\alpha_j)_{i,j=1,\ldots,n}\big)\Big)^2$.

III-10 $\beta_i = \sum_{p=1}^{n} A_{i,p}\alpha_p$ entraine pour tout j : $\sigma_j(\beta_i) = \sum_{p=1}^{n} A_{i,p}\sigma_j(\alpha_p)$; la matrice $B' = \big(\sigma_j(\beta_i)\big)$ est donc AB (avec la notation de la question précédente). Par suite et en appliquant deux fois la question précédente : $D(\beta_1, \ldots, \beta_n) = (\det B')^2 = (\det(AB))^2 = (\det A \det B)^2 = (\det A)^2(\det B)^2 = (\det A)^2 D(\alpha_1, \ldots, \alpha_n)$

III-11 $\sigma_i(\theta^j) = (\sigma_i(\theta))^j$ donc $\det\big(\sigma_i(\theta^j)\big)_{1\le i\le n, 0\le j\le n-1}$ est le déterminant de Vandermonde $V(\sigma_1(\theta), \ldots, \sigma_n(\theta))$ qui vaut $\prod_{1\le j<i\le n} \big(\sigma_i(\theta) - \sigma_j(\theta)\big)$. C'est aussi, puisqu'il y a $n(n-1)/2$ facteurs, en changeant tous les signes : $(-1)^{n(n-1)/2} \prod_{1\le j<i\le n} \big(\sigma_j(\theta) - \sigma_i(\theta)\big) = (-1)^{n(n-1)/2} \prod_{1\le i<j\le n} \big(\sigma_i(\theta) - \sigma_j(\theta)\big)$.
Faisant le produit des deux expressions :
$D(1, \theta, \theta^2, \ldots, \theta^{n-1}) = V(\sigma_1(\theta), \ldots, \sigma_n(\theta))^2 = (-1)^{n(n-1)/2} \prod_{\substack{1\le i,j\le n \\ i\ne j}} \big(\sigma_i(\theta) - \sigma_j(\theta)\big)$

III-12 Posons $\alpha_i = \sum_{p=0}^{n-1} A_{i,p}\theta^p$. Comme $(1, \theta, \ldots, \theta^{n-1})$ est une $\mathbf{Q}$-base de K, $(\alpha_1, \ldots, \alpha_n)$ est une $\mathbf{Q}$-base de K si et seulement si la matrice $A = \big(A_{i,j}\big)_{1\le i,j\le n}$ est inversible.
Or on a d'après la question **10** : $\quad D(\alpha_1, \ldots, \alpha_n) = (\det A)^2 D(1, \theta, \ldots, \theta^{n-1})$ $\quad$ et d'après la question **11** $D(1, \theta, \ldots, \theta^{n-1}) \ne 0$ (tous les $\sigma_i(\theta)$ sont distincts d'après la deuxième partie). Par suite A inversible équivaut à $\det A \ne 0$ et encore à $D(\alpha_1, \ldots, \alpha_n) \ne 0$.
Conclusion : $\quad (\alpha_1, \ldots, \alpha_n)$ est une $\mathbf{Q}$-base de K si et seulement si $D(\alpha_1, \ldots, \alpha_n)$ est non nul.

III-13.a $\phi = X^3 - X - 1$ a pour dérivée $3X^2 - 1$ nulle en $\pm\frac{1}{\sqrt{3}}$. Sur $]-\infty, -\frac{1}{\sqrt{3}}]$ $\quad \phi$ croit de $-\infty$ à $\phi(-\frac{1}{\sqrt{3}}) = \frac{2}{3\sqrt{3}} - 1 < 0$, sur $[-\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}]$ $\quad \phi$ est décroissante strictement négative, et sur $[\frac{1}{\sqrt{3}}, +\infty]$ $\quad \phi$ est strictement croissante continue depuis $\phi(\frac{1}{\sqrt{3}}) < 0$ jusqu'à $+\infty$ donc admet une racine θ unique. Il en résulte que θ est l'unique racine réelle de $X^3 - X - 1$.

III-13.b Le polynôme $\mathbf{Q}$ minimal de θ est $\phi = X^3 - X - 1$.
Il suffit pour le prouver de montrer que ϕ est irréductible. Sinon ϕ serait produit dans $\mathbf{Q}[X]$ de deux polynômes non constants dont l'un serait de degré 1 : ϕ aurait une racine rationnelle $\frac{p}{q}$ (fraction

irréductible). On aurait $p^3 - pq^2 - q^3 = 0$ donc q diviseur de p^3 et premier à p^3 : donc $q = 1$. Alors $p^3 - p - 1 = 0$ entraine p divise 1 donc $p = \pm 1$: on vérifie que 1 et -1 ne sont pas racines de ϕ. Donc ϕ n'est pas réductible sur $\mathbf{Q}$.

III-13.c Soit $\theta_1 = \theta$, θ_2 et θ_3 les racines de ϕ.
D'après la deuxième partie la liste des $\sigma_i(\theta)$ est la liste des θ_i.
On a donc en utilisant directement la question **11** sous la forme "carré du Vandermonde" :

$$D(1, \theta, \theta^2) = (\theta 2 - \theta_1)^2(\theta_3 - \theta_1)^2(\theta_3 - \theta_2)^2.$$

On obtient dans l'équation $\phi = 0$: $\theta_1 + \theta_2 + \theta_3 = 0$ et $\theta_1\theta_2\theta_3 = 1$.
Par suite $(\theta_2 - \theta_3)^2 = (\theta_1 + \theta_2)^2 - 4\theta_1\theta_2 = \theta_3^2 - \frac{4}{\theta_3} = \frac{1}{\theta_3}(\theta_3^3 - 4) = \frac{1}{\theta_3}(\theta_3 - 3)$.
La situation étant ici symétrique entre les différentes racines on a :

$$D(1, \theta, \theta^2) = \prod_{i=1}^{3} \frac{\theta_i - 3}{\theta_i} = \prod_{i=1}^{3} (\theta_i - 3)$$

C'est donc le produit des racines de l'équation dont les racines sont les $u_i = \theta_i - 3$. Posant $u = X - 3$ donc $X = u + 3$ on obtient l'équation $(u + 3)^3 - (u + 3) - 1 = 0$; le terme constant est $3^3 - 3 - 1 = 23$ et le produit des racines est donc -23.
Il en résulte $D(1, \theta, \theta^2) = -23$.

En fait ceci vaut pour l'une quelconque des racines θ_i : il est inutile de spécifier qu'il s'agit de la racine réelle. Comme le montre bien la question 11 le résultat est symétrique entre les différentes racines. En dissymétrisant l'énoncé induisait ici à faire des calculs plus lourds.