DM n°8

EXERCICE 1

Soit la série entière de la variable complexe z, $\sum_{n\geq 1}^{+\infty} \frac{z^n}{\sqrt{n}}$.

1. Donner le rayon de convergence de cette série entière. On note f sa somme.
2. Déterminer l'ensemble Z des complexes z pour lesquels l'application
$$u \mapsto \frac{1}{e^{u^2} - z}$$
est intégrable sur $]0, +\infty[$. Soit
$$g \,:\, Z \to \mathbf{C}\,;\; z \mapsto \frac{2z}{\sqrt{\pi}} \int_0^{+\infty} \frac{\mathrm{d}u}{e^{u^2} - z}.$$
3. Montrer que f et g coïncident sur $\{z \in \mathbf{C} |\; |z| < 1\}$.
4. Montrer que $f(e^{i\theta}) = g(e^{i\theta})$, pour tout $\theta \in]0, 2\pi[$.

PROBLÈME

Les deux premières parties sont consacrées à l'étude d'extensions du corps $\mathbf{Q}$, c'est-à-dire de sur-corps de $\mathbf{Q}$. La troisième partie définit de façon abstraite la construction d'extentions d'un corps quelconque. La quatième partie étudie les corps finis en utilisant notamment les résultats de la partie précédente, enfin le devoir s'achève par le dénombrement de polynômes iréductibles sur $\mathbf{Z}/p\mathbf{Z}$, permettant de prouver un résultat admis dans la quatrième.

Première partie : Un exemple d'extension du corps $\mathbf{Q}$

1. Soit P le polynôme $X^3 - X - 1$.
Montrer que P n'a pas de racines rationnelles. En déduire que P est irréductible dans $\mathbf{Q}[X]$.
Montrer que P a une racine réelle que l'on notera ω.
2. Soit $\mathbf{K}$ le $\mathbf{Q}$-espace vectoriel engendré par $(\omega^i)_{i\in\mathbf{N}}$.
Montrer que $\mathbf{K}$ est de dimension finie, et donner une base simple de K.
3. Montrer que $\mathbf{K}$ est une $\mathbf{Q}$-sous-algèbre de $\mathbf{R}$, muni de sa structure naturelle de $\mathbf{Q}$-algèbre.
4. Montrer que $\mathbf{K}$ est un sous-corps de $\mathbf{R}$.

Deuxième partie : Cas général d'extension de $\mathbf{Q}$
Soit a un réel.

1. Montrer que tout sous-corps de $\mathbf{R}$ contient $\mathbf{Q}$.
2. Montrer que l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a admet un plus petit élément pour l'inclusion. On le notera dans la suite $\mathbf{Q}(a)$.
3. Montrer que $\phi \,:\, \mathbf{Q}[X] \to \mathbf{R}\,;\; P \mapsto P(a)$ est un morphisme de la $\mathbf{Q}$-algèbres $\mathbf{Q}[X]$ dans la $\mathbf{Q}$ algèbre $\mathbf{R}$. On note $\mathbf{Q}[a]$ son image.

4. Soit $I := \{P \in \mathbf{Q}[X], P(a) = 0\}$. Montrer que I est un idéal de $\mathbf{Q}[X]$.
5. Le réel a est dit algébrique (sur $\mathbf{Q}$), si, par définition, a est racine d'un polynôme non nul à coefficients entiers.
   Montrer que a est algèbrique si et seulement si I est non réduit à $\{0\}$.
   Dans cette partie on suppose dans la suite que que a est algèbrique, sauf à la dernière question.
6. Montrer qu'il existe un et un seul élément de $\mathbf{Q}[X]$ unitaire, μ_a, tel que $I = \mu_a\mathbf{Q}[X]$.
   Montrer que μ_a est irréductible dans $\mathbf{Q}[X]$. Montrer que si a est irrationnel, alors le degré de μ_a est supérieur ou égal à 2. Déterminer μ_a pour $a = \sqrt{2}$ et pour $a = \sqrt{\frac{1+\sqrt{5}}{2}}$.
7. Montrer que $\mathbf{Q}[a]$ est un corps. Montrer que $\mathbf{Q}(a) = \mathbf{Q}[a]$.
   Montrer que $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension n, où n est le degré de μ_a, dont on donnera une base simple.
8. Si a est non algébrique, montrer qu'alors $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension infinie [1].

Troisième partie : Extension de corps **FACULTATIF**

$\mathbf{K}$ désigne un corps et P_0 un élément de $\mathbf{K}[X]$ *irréductible*. On rappelle qu'un élément P de $\mathbf{K}[X]$ est irréductible si :

— il est non inversible ;

— pour tout couple (A, B) d'éléments de $\mathbf{K}[X]$, tel que $P = AB$, A ou B est inversible.

Enfin $\mathfrak{I}$ désignera l'idéal engendré par P_0,

$$\mathfrak{I} = P_0\mathbf{K}[X]$$

On définit sur $\mathbf{K}[X]$ la relation $\mathcal{R}$ définie par : pour tout P et tout Q éléments de $\mathbf{K}[X]$, $P\mathcal{R}Q$ si $P - Q \in \mathfrak{I}$.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
   On notera $\bar{P}$ la classe d'équivalence d'un élément P de $\mathbf{K}[X]$ et $\mathbf{K}[X]/\mathfrak{I}$ l'ensemble des classes d'équivalences.
2. Montrer que l'on peut définir deux lois internes $+$ et $\times$ sur $\mathbf{K}[X]/\mathfrak{I}$ telles que pour tout couple (P, Q) d'éléments de $\mathbf{K}[X]$
   $$\bar{P} + \bar{Q} = \overline{P + Q} \text{ et } \bar{P} \times \bar{Q} = \overline{P \times Q}$$
3. Montrer sommairement que $(\mathbf{K}[X]/\mathfrak{I}, +, \times)$ est un anneau commutatif et que l'application
   $$\pi : \mathbf{K}[X] \to \mathbf{K}[X]/\mathfrak{I}\,;\ P \mapsto \bar{P}$$
   est un morphisme d'anneaux
4. Montrer que $\mathbf{K}[X]/\mathfrak{I}$ peut être muni d'une structure de $\mathbf{K}$-algèbre qui fasse de π un morphisme d'algèbres.
5. Déterminer la dimension de la $\mathbf{K}$-algèbre $\mathbf{K}[X]/\mathfrak{I}$ en fonction du degré de P_0 et en donner une base.
6. *Exemple* — Dans cette question on prend pour $\mathbf{K}$ le corps des réels et pour P_0 le polynôme $X^2 + 1$. A quel corps est isomorphe $\mathbf{R}[X]/\mathfrak{I}$

1. On pourrait montrer que $\mathbf{Q}(a)$ est isomorphe en tant que corps au corps $\mathbf{Q}(X)$.

Quatrième partie : CORPS FINIS

Soit $(\mathbf{F}, +, \times)$ un corps. On note $1_{\mathbf{F}}$ l'unité de $\mathbf{F}$ et pour tout entier k et tout élément a de $\mathbf{F}$, $k \cdot a$, désigne l'élément $\underbrace{a + a + \cdots + a}_{k \text{ termes}}$ pour $k \geq 1$, l'élément $\underbrace{(-a) + (-a) + \cdots + (-a)}_{-k \text{ termes}}$ pour $k \leq -1$ et enfin $1_{\mathbf{F}}$ pour $k = 0$

On admet le résultat élémentaire et au programme de MP suivant :

L'application

$$\varphi \ : \ \mathbf{Z} \to \mathbf{F} \, ; \ k \mapsto k \cdot 1_{\mathbf{F}}$$

est un morphisme d'anneaux.

Son noyau est donc un sous-groupe de $(\mathbf{Z}, +)$, donc de la forme pZ, où p désigne un élément de $\mathbf{N}$. L'entier naturel p s'appelle caractéristique de $\mathbf{F}$.

1. Montrer que si p est nul alors $\mathbf{F}$ est infini.

   Dans toute la suite on supposera que F est fini, donc que p est non nul.

2. Montrer qu'il existe une et une seule application $\tilde{\varphi}$ de $\mathbf{Z}/p\mathbf{Z}$ dans $\mathbf{F}$ tel que $\varphi = \tilde{\varphi} \circ \pi_p$, où π_p désigne la surjection (dite canonique) de $\mathbf{Z}$ sur $Z/p\mathbf{Z}$, qui à un entier x associe sa classe modulo p.
3. Montrer que $\tilde{\varphi}$ est un morphisme d'anneaux injectif.
4. On note $\mathbf{k} = \tilde{\varphi}(\mathbf{Z}/p\mathbf{Z})$. Montrer que $\mathbf{k}$ est un sous-anneau de $\mathbf{F}$ isomorphe à $\mathbf{Z}/p\mathbf{Z}$. En déduire que p est un nombre premier.
5. Montrer que $\mathbf{k}$ est le plus petit sous-corps de $\mathbf{F}$.

   Le sous-corps $\mathbf{k}$ est appelé sous corps premier de $\mathbf{F}$, on vient de voir qu'il est isomorphe à $\mathbf{Z}/p\mathbf{Z}$
6. En munissant $\mathbf{F}$ d'une structure d'espace vectoriel sur $\mathbf{k}$, montrer que le cardinal de $\mathbf{F}$ est une puissance de p.

La fin est réservée aux élèves préparant l'X ou les ÉNS.

On se propose d'étudier la réciproque. On admettra le théorème suivant :

Théorème : *Tout corps* $\mathbf{K}$ *admet un sur-corps* $\bar{\mathbf{K}}$ *tel que l'on ait :*

— $\bar{\mathbf{K}}$ *est algébriquement clos* ;

— *Tout élément de* $\bar{\mathbf{K}}$ *est racine d'un polynôme à coefficients dans* $\mathbf{K}$ *on dit est algébrique sur* $\mathbf{K}$.

Un tel sur-corps $\bar{\mathbf{K}}$ *est appelé cloture algébrique de* $\mathbf{K}$.

On a l'unicité de la cloture algébrique, en ce sens que deux clotures algébriques de $\mathbf{K}$ *sont des corps isomorphes par un isomorphisme induisant sur* $\mathbf{K}$ *l'identité. On parle donc de* LA *cloture algébrique d'un corps.*

Par exemple $\mathbf{C}$ *est la cloture algébrique de* $\mathbf{R}$.

Dans la suite p désigne un nombre premier, $\mathbf{F}_p$ désignera le corps $\mathbf{Z}/p\mathbf{Z}$ et n un entier naturel non nul. On pose $q = p^n$ et l'on va étudier l'existence d'un corps à q éléments.

7. On suppose provisoirement qu'il existe un élément de $\mathbf{F}_p[X]$ irréductile de degré n.

   (a) Montrer en utilisant la partie précédente qu'il existe un corps à q élément $\mathbf{F}_q$ qui soit une $\mathbf{F}_p$ algèbre. Quelle est la caractéristique de $\mathbf{F}_q$. Dans la suite on identifira un élément a de $\mathbf{F}_p$ et l'élément $a \cdot 1_{\mathbf{F}_q}$, (1_{F_q} est l'unité de $\mathbf{F}_q$). En particulier on identifira $1_{\mathbf{F}_q}$ et l'élément de $\bar{1}$ de $\mathbf{F}_p$ et le sous-corps $\mathbf{F}_p \cdot 1_{\mathbf{F}_q}$ et $\mathbf{F}_p$.

   (b) Montrer que $f \ : \ \mathbf{F}_q \to \mathbf{F}_q \, ; \ x \mapsto x^p$ est morphisme de corps, on l'appelle morphisme de Frobenius.

(c) Montrer que tout élément x de $\mathbf{F}_q$ vérifie $x^q = x$.

(d) Montrer que $\mathbf{F}_q$ est l'ensemble des racines du polynôme $X^q - X$ qui est un élément de $\mathbf{F}_q[X]$ à coefficients dans $\mathbf{F}_p$.

On ne suppose plus l'existence d'un élément de $\mathbf{F}_p[X]$ irréductile de degré n.

8. Montrer que $\bar{\mathbf{F}}_p$ admet un et un seul sous-corps à q éléments, on le notera $\mathbf{F}_q$. On étudira le polynôme $X^q - X$.

9. On se propose de montrer qu'il existe un un élément de $\mathbf{F}_p[X]$ irréductile de degré p. Soit le l'élément de $\mathbf{F}_p[X]$, $P_0 = X^p - X - 1$. Et soit α une racine de P_0 dans $\bar{\mathbf{F}}_p$ la cloture algébrique de $\mathbf{F}_p$.

(a) Montrer que l'ensemble des racines de P_0 est $\{\alpha, \alpha + \bar{1}, \ldots, \alpha + \overline{p-1}\}$

(b) Montrer que P_0 est irréductible.

(c) Expliciter la structure du corps $\mathbf{F}_4$ ($p = 2, n = 2$).

Cinquième partie : Polynômes irréductibles de $\mathbf{F}_p[X]$

1. Montrer que pour tout entier naturel $m \geq 1$, $\mathbf{F}_{p^m}$ est un sous-corps de $\mathbf{F}_{p^n}$ si et seulement si m divise n.

2. *Formule d'inversion de Moebius* —
Pour tout élément n de $\mathbf{N}^*$, $\mathcal{D}_n$ désigne l'ensemble des diviseurs positifs de n. On munit $\mathcal{F}(\mathbf{N}^*, \mathbf{Z})$, ensemble des applications de $\mathbf{N}^*$ dans $\mathbf{Z}$, de la loi de composition interne $\star$ définie par,
$$f \star g \ : \ \mathbf{N}^* \to \mathbf{Z} \, ; \ n \mapsto \sum_{d \in \mathcal{D}_n} f(d) g\left(\frac{n}{d}\right),$$
pour tout couple (f, g) d'éléments de $\mathcal{F}(\mathbf{N}^*, \mathbf{Z})$.

(a) Montrer que la loi $\star$ est commutative, associative et admet pour élément neutre l'application
$$e \ : \ \mathbf{N}^* \to \mathbf{Z} \, ; \ n \mapsto \begin{cases} 1, & \text{pour } n = 1, \\ 0, & \text{sinon.} \end{cases}$$

(b) Soit l'application μ de $\mathbf{N}^*$ dans $\mathbf{Z}$ définie ainsi :
— $\mu(1) = 1$,
— pour tout entier $n \geq 2$ de décomposition en facteurs premiers $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, où les α_i, $i = 1 \ldots k$ sont non nuls $\mu(n)$ vaut zéro si l'un des α_i est supérieure ou égal à 2 et $\mu_n = (-1)^k$ si tous les α_i sont égaux à 1.
Montrer que
$$\sum_{d \in \mathcal{D}_n} \mu(d) = \begin{cases} 1 & \text{pour } n = 1, \\ 0 & \text{sinon.} \end{cases}$$

(c) Soient f et g des applications de $\mathbf{N}^*$ dans $\mathbf{Z}$ telles que pour tout entier $n \geq 1$,
$$g(n) = \sum_{d \in \mathcal{D}_n} f(d).$$
Déduire des questions précédentes que pour tout $n \in \mathbf{N}^*$,
$$f(n) = \sum_{d \in \mathcal{D}_n} \mu\left(\frac{n}{d}\right) g(d).$$

Remarque : Cette formule donne pour tout entier $n \geq 1$, d'exprimer $\varphi(n)$, (φ désigne de l'indicatrice d'Euler) :

$$\varphi(n) = \sum_{d \in \mathcal{D}_n} d\mu\left(\frac{n}{d}\right).$$

Pour tout entier $m \geq 1$, I_m désigne le nombre de polynômes, de $\mathbf{F}_p[X]$ irréductibles, unitaires, de degré m.

3. Par n on désigne toujours un entier naturel non nul. Soit Q un facteur irréductible de $X^{p^n} - X$ de degré d et α une racine de Q dans $\bar{\mathbf{F}}_p$. Montrer que le $\mathbf{F}_p$-espace vectoriel engendré par $(\alpha,^0, \alpha^1 \ldots, \alpha^{d-1})$ est un sous-corps de $\mathbf{F}_{p^n}$ et un espace vectoriel de dimension d. En déduire que $d|n$ et $\alpha \in \mathbf{F}_{p^n}$.
4. Soit Q' un polynôme irréductible de $\mathbf{F}_p$ dont le degré d divise n. Montrer que Q' divise $X^{p^n} - X$.
5. Prouver que :

$$p^n = \sum_{d \in \mathcal{D}_n} dI_d.$$

En déduire que :

$$I_n = \frac{1}{n} \sum_{d \in \mathcal{D}_n} \mu\left(\frac{n}{d}\right) p^d.$$

6. En déduire qu'il existe au moins un polynôme irréductible de $\mathbf{F}_p$ de degré n.

Indications pour le DM n°8 8

Extensions de corps

EXERCICE

1. La série de Riemann $\sum_{n\geq 1}\frac{1^n}{\sqrt{n}}$ ne converge pas absolument donc $R\leq 1$; cette série ne diverge pas grossièrement, donc $R\geq 1$. Au total : $R=1$.
2. Soit $z\in\mathbf{C}$. L'intégrabilité de $u\mapsto\frac{1}{\mathrm{e}^{u^2}-z}$ sur $]0,+\infty[$ exige (pour respecter le programme) que cette application soit définie et continue par morceaux sur $]0,+\infty[$. Comme l'exponentiel induit une bijection de $\mathbf{R}_+^*$ sur $]1,+\infty[$, si $u\mapsto\frac{1}{\mathrm{e}^{u^2}-z}$ est intégrable sur $]0,+\infty[$, alors z n'est pas élément de $]1,+\infty[$.
   Suposons inversement : $z\notin]1,+\infty[$.
   L'intégrabilité au voisinage de $+\infty$ est enfantine
   Si $z\neq 1$ celle au voisinage de 0 est triviale. Si $z=1$ On montre par équivalence à une fonction de référence lé non intégrabilité.
   Concluons : $Z=\mathbf{C}\setminus[1,+\infty[$.
3. Soit z un élément du disque ouvert unité de $\mathbf{C}$ (qui est bien inclus dans Z, ouf !).
   Posons $h\ :]0,+\infty[\to\mathbf{R}\,;\ u\mapsto\frac{z}{\mathrm{e}^{u^2}-z}$ et pour $n\in\mathbf{N}^*$, $f_n;]0,+\infty[\to\mathbf{C}\,;\ u\mapsto z^n(\mathrm{e}^{-u^2})^n$, ainsi la série $\sum_{n\geq 1}f_n$ converge simplement et a pour somme h. Notons que tant les f_n que f sont continues.
   On peut sans se posser de questions utiliser le théorème d'interversion séries/intégrale
4. On peut constater que le théorème d'interversion séries/intégrale ne marche plus pour z de module 1. On utilise le cours de terminale qui explicite le reste.
   Soit $\theta\in]0,2\pi[$ et $z=\mathrm{e}^{i\theta}$ Gardons les notations de 3,

$$h=\sum_{n=1}^{N}f_n+\frac{z^{N+1}\mathrm{e}^{-(N+1)u^2}}{1-z\mathrm{e}^{-u^2}},$$

   et donc par linéarité de l'intégrale de fonctions intégrables :

$$g(z)=\sum_{n=1}^{N}\frac{z^n}{\sqrt{n}}+\frac{2}{\sqrt{\pi}}\int_0^{+\infty}\frac{z^{N+1}\mathrm{e}^{-(N+1)u^2}}{1-z\mathrm{e}^{-u^2}}\mathrm{d}u.$$

   Reste à faire tendre le reste vers 0....on pourra remarquer que $:]0,+\infty[\,;u\mapsto|1-z\mathrm{e}^{-u^2}|$ est minorée par un réel strictement positif..

Problème

Première partie

1. Montrons que P est irréductible dans $\mathbf{Q}[X]$. En premier lieu P n'est pas inversible. Ensuite, supposons que P s'écrive $P=AB$, avec A et B éléments de $\mathbf{Q}[X]$. Alors $\mathrm{d}^\circ A+\mathrm{d}^\circ B=\mathrm{d}^\circ P$. Or ni A ni B ne sont de degré 1....

   Le polynôme P est de degré *impair* à coefficients *réels*, il admet donc une racine réelle ω.

2.

3. • K sous-espace vectoriel sur Q de $\mathbf{R}$ est *stable par combinaison linéaire.*
   • soient x et x' des éléments de K. Il existe des rationnels a, b, c, a', b', c' tels que $x = a\omega^2 + b\omega + c,\ x' = a'\omega^2 + b'\omega + c'$. Alors...
   Donc $xx' \in \underset{\mathbf{Q}}{\text{vect}}(\omega^i)_{i\in\mathbf{N}} = K$. Donc K *est stable par produit.*
   • Enfin $1 = \omega^0 \in K$.
   De ces trois points on déduit : K est une $\mathbf{Q}$-sous-algèbre de $\mathbf{R}$.
4. D'après (c), K est un sous-anneau de $\mathbf{R}$, il est donc *commutatif* et *non trivial.*
   Soit, par ailleurs, x un élément non nul de K. Il existe, d'après (b), des rationnels a, b et c non tous nuls, tels que $x = a\omega^2 + b\omega + c$. Soit $D = aX^2 + bX + C$. P et D sont, dans $Q[X]$, premiers entre eux, . *L'inverse de x est donc élément de K.*
   Conclusion : K est un sous-corps de $\mathbf{R}$.

Deuxième partie Cas général :

Soit a un réel.

1. Soit K_0 un sous-corps de $\mathbf{R}$. Il contient 1, donc, étant stable par somme et différence il contient $\mathbf{Z}$. K_0 étant stable par passage à l'inverse et multiplication il contient $\mathbf{Q}$.
2. Raisonner comme dans la preuve de l'existence d'un sous groupe engendré en considérant l'ensemble $\mathcal{K}$ des sous-corps de $\mathbf{R}$ qui contiennent a,
3. Soient P et Q des éléments de $\mathbf{Q}[X]$, λ et μ des rationnels.
   Donc ϕ est un morphisme de la $\mathbf{Q}$-algèbre $\mathbf{Q}[X]$ dans la $\mathbf{Q}$-algèbre $\mathbf{R}$.
4. D'après la question précédente, ϕ induit notamment un morphisme de l'anneau $\mathbf{Q}[X]$ sur l'anneau $\mathbf{R}$. I en est le *noyau*, c'est donc un idéal de $\mathbf{Q}[X]$.
5. Que a soit algèbrique si et seulement si I est non réduit à $\{0\}$ est presque évident.
6. C'est du cours.

   $\mu_a(a) = 0$, donc μ_a ne saurait être un inversible de $\mathbf{Q}[X]$. Soient A et B des éléments de $\mathbf{Q}[X]$, tels que $\mu_a = AB$. Reste à montrer que cette décomposition est triviale.

   Supposons que $\mathrm{d}^\circ\mu_a \leq 1$. $\mathrm{d}^\circ\mu_a \neq -\infty$ (I non nul) et $\mathrm{d}^\circ\mu_a \neq 0$ car $\mu_a(a) = 0$, donc $\mathrm{d}^\circ\mu_a = 1$. montrer qu'alors $a \in \mathbf{Q}$.

   L'élément de $\mathbf{Q}[X]$, $X^2 - 2$ admet $\sqrt{2}$ comme racine. Donc $X^2 - 2 | \mu_{\sqrt{2}}$. Or $\sqrt{2}$ est notoirement irrationnel donc, comme on vient de le voir, $\mathrm{d}^\circ\mu_{\sqrt{2}} \geq 2$. Donc $X^2 - 2$ qui est unitaire est égal à $\mu_{\sqrt{2}}$.

   $$\underline{\mu_{\sqrt{2}} = X^2 - 2.}$$

   Maintenant $a = \sqrt{\frac{1+\sqrt{5}}{2}}$. L'élément de $\mathbf{Q}[X]$, $X^4 - X^2 - 1$ admet a comme racine. Donc $\mu_a | X^4 - X^2 - 1$. Montrons que $X^4 - X^2 - 1$ est irréductible dans $\mathbf{Q}[X]$. Supposons qu'il existe A et B éléments de $\mathbf{Q}[X]$ tels que :

   $$X^4 - X^2 - 1 = AB.$$

   En notant $a' = \sqrt{\frac{-1+\sqrt{5}}{2}}$. $X^4 - X^2 - 1$ admet quatre racines complexes, $a, -a, ia', -ia'$. $\sqrt{5}$ étant irrationnel, on montre qu'aucune de ses racines n'est rationnelle, donc ni A ni B n'est de degré 1. Supposons que $\mathrm{d}^\circ A = 2$ et donc $\mathrm{d}^\circ B = 2$.

L'un des deux polynômes A et B, disons pour fixer les idées A, admet ia' comme racine etc....

$$\underline{\mu_a = X^4 - X^2 - 1}.$$

7. $\mathbf{Q}[a]$ est l'image par le morphisme d'anneaux ϕ de l'anneau $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-anneau* de $\mathbf{R}$. Comme $\mathbf{R}$ est un corps, l'anneau $\mathbf{Q}[a]$ est *commutatif et non trivial.* Soit x un élément non nul de $\mathbf{Q}[a]$. Il existe $P \in \mathbf{Q}[X]$ tel que $x = P(a)$. On montre comme dans l'exemple que $x^{-1} \in \mathbf{Q}[a]$. Autrement dit $\mathbf{Q}[a]$ est *stable par passage à l'inverse.*

   CONCLUSION : $\underline{\mathbf{Q}[a] \text{ est un corps.}}$

   $\mathbf{Q}[a]$ est un corps qui contient a. Donc $\mathbf{Q}(a) \subset \mathbf{Q}[a]$

   Soit Soit x un élément de $\mathbf{Q}[a]$. Il sécrit

$$x = \sum_{i=0}^{n} c_i a^i,$$

   avec n un naturel et $c_0, c_1, \ldots, c_n$ des rationnels. Montrer que $x \in \mathbf{Q}(a)$...

   CONCLUSION : $\underline{\mathbf{Q}(a) = \mathbf{Q}[a]}$. $\mathbf{Q}[a]$ est l'image par ϕ, morphisme de $\mathbf{Q}$-espaces vectoriels, de l'espace vectoriel $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-espace vectoriel* du Q-espace vectoriel $\mathbf{R}$.Comme dans l'exemple on montre que la famille *la famille* $(a^0, a^1, \ldots, a^{n-1})$ *est une base de* $\mathbf{Q}[a]$.
   Finalement $\underline{(a^0, a^1, \ldots, a^{n-1}) \text{ est une base de } \mathbf{Q}[a], \text{ qui est donc de dimension } n}$.

8. Supposons que la famille $(a_i)_{i \in \mathbf{N}}$ soit liée. Montrons qu'alors a est algèbrique. Par hypothèse il existe $m \in \mathbf{N}$, $\lambda_0, \lambda_1, \ldots, \lambda_{m-1}$ des rationnels non tous nuls, tels que : $\lambda_0 a^0 + \lambda_1 a^1 + \cdots + \lambda_{m-1} a^{m-1} = 0$. Soit l'élément de $\mathbf{Q}[X]$,

$$D = \lambda_0 X^0 + \lambda_1 X^1 + \cdots + \lambda_{m-1} X^{m-1}.$$

   D est non nul et $D \in I$, donc d'après 5., a est algébrique. Par contraposée, si a est non algébrique, alors la famille d'éléments de $\mathbf{Q}(a)$, $(a_i)_{i \in \mathbf{N}}$ est libre et donc $\underline{\mathbf{Q}(a) \text{ est de dimension infinie}}$.