DM n^o 19

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 $\left(\omega^i\right)_{i\in\mathbf{N}}$.
   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

$\mathbf{K}$ 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.

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

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 $\mathbf{R}[X]/\mathfrak{I}$

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.

   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.

Correction du DM n°1 bis

Extensions de corps

Première partie

1. Soit P le polynôme $X^3 - X - 1$.
   Supposons que P ait une racinne rationnelle r. Elle s'écrit : $r = \frac{p}{q}$ avec $p \in \mathbf{Z}$, $q \in \mathbf{N}$ et p et q premiers entre eux. On a donc : $r^3 - r - 1 = 0$, Soit

   $$p^3 - pq^2 - q^3 = 0. \tag{1}$$

   On déduit de cette égalité que p divise q^3. Or p et q sont premiers entre eux donc le théorème de Gauß dit que p divise q^2. Une nouvelle application du thèorème de gauß donne que p divise q, enfin une dernière application de ce théorème donne que p divise 1. Donc :

   $$p = 1. \tag{2}$$

   On déduit aussi de (1) que q divise p^3. Un raisonnement analogue au précédent donne $q|1$. Donc

   $$q = \pm 1. \tag{3}$$

   Donc on déduit de (2–3), que les seules racines rationnelles possibles sont 1 et -1. Or $P(1) = -1$, $P(-1) = -1$. Donc P n'admet pas de racines rationnelles.

   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, car un élément de $\mathbf{Q}[X]$ de degré 1 admet une racine rationnelle et P n'en admet pas. Donc $\mathrm{d}^\circ A = 0$ et $\mathrm{d}^\circ B = 3$ où $\mathrm{d}^\circ B = 0$ et $\mathrm{D}^\circ A = 3$.
   En conclusion P est irréductible dans $\mathbf{Q}[X]$.

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

2. Soit c un élément de $\mathbf{K}$. Par définition de $\mathbf{K}$, il existe un entier naturel n et des rationnels $a_0, a_1, \ldots, a_n$ tels que : $c = \sum_{i=0}^{n} a_i \omega^i$. Soit l'élément de $\mathbf{Q}[X]$, $C = \sum_{i=0}^{n} a_i X^i$. Par division euclidienne de C par P dans $\mathbf{Q}[X]$ on obtient :

   $$C = QP + rX^2 + sX + t, \tag{4}$$

   avec $Q \in \mathbf{Q}[X]$, r, s et t des rationnels. En substituant ω à l'indéterminée dans (4), il vient : $c = C(\omega) = Q(\omega)P(\omega) + r\omega^2 + s\omega + t = r\omega^2 + s\omega + t$. Donc c étant quelconque, on a : $\mathbf{K}$ est le Q-espace vectoriel engendré par la sous famille de $(\omega^i)_{i\in\mathbf{N}}$, $(\omega^0, \omega^1, \omega^2)$.

   Montrons que la famille $(\omega^0, \omega^1, \omega^2)$ est libre. Soit λ, μ et ν des rationnels tels que : $\lambda\omega^2 + \mu\omega + \nu = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda X^2 + \mu X + \nu$. Supposons C non nul. Alors par division euclidienne : $P = \tilde{Q}C + uX + v$ avec $\tilde{Q} \in \mathbf{Q}[X]$, u et v des rationnels. En substituant dans cette égalité ω à l'indéterminée, il vient $0 = u\omega + v$. Comme ω est irrationnel $u = 0$ et donc $v = 0$, et donc C divise P. Mais P étant irréductible C est constant non nul, ce qui contredit $C(\omega) = 0$. Donc C est nul, c'est-à-dire : $\lambda = \mu = \nu = 0$. D'où la liberté de $(\omega^0, \omega^1, \omega^2)$.

   Finalement $(\omega^0, \omega^1, \omega^2)$ est une base de K.

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

     $$xx' = aa'\omega^4 + (ab' + a'b)\omega^3 + (ac' + a'c + bb')\omega^2 + (bc' + c'b)\omega + cc'.$$

     Donc $xx' \in \underset{\mathbf{Q}}{\mathrm{vect}}(\omega^i)_{i\in\mathbf{N}} = K$. 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, en effet P est irréductible (cf. 1.) et ne divise pas D, puisque $\mathrm{d}^\circ P > \mathrm{d}^\circ D > -\infty$. Le lemme de Bezout assure donc l'existence de U et V éléments de $\mathbf{Q}[X]$ tels que : $UD + VP = 1$. En substituant ω à l'indéterminée X dans cette égalité, il vient :

$$U(\omega)D(\omega) + V(\omega)P(\omega) = xD(\omega) = 1.$$

   Donc $D(\omega)$ est l'inverse de x. *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. Soit $\mathcal{K}$ l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a. Soit $\mathbf{Q}(a)$, l'intersection de tous les éléments de $\mathcal{K}$:

$$\mathbf{Q}(a) = \bigcap_{K \in \mathcal{K}} K.$$

   - $\mathbf{Q}(a)$ est un sous-corps de $\mathbf{R}$ comme intersection non vide ($\mathbf{R} \in \mathcal{K}$) de sous-corps.
   - Pour tout élément K de $\mathcal{K}$, $a \in K$, donc $a \in \mathbf{Q}(a)$.
   - Soit K_0 un sous-corps de $\mathbf{R}$ qui contient a, par définition de $\mathcal{K}$, $K_0 \in \mathcal{K}$ donc

$$\mathbf{Q}(a) = \bigcap_{K \in \mathcal{K}} K \subset K_0.$$

   Donc l'ensemble $\mathcal{K}$ des sous-corps de $\mathbf{R}$ qui contiennent a,
   admet $\mathbf{Q}(a)$ comme plus petit élément pour l'inclusion.
3. Soient P et Q des éléments de $\mathbf{Q}[X]$, λ et μ des rationnels.
   - $\phi(\lambda P + \mu Q) = (\lambda P + \mu Q)(a) = \lambda P(a) + \mu Q(a) = \lambda\phi(P) + \mu\phi(Q)$.
   - $\phi(P \times Q) = (P \times Q)(a) = P(a) \times Q(a) = \phi(P) + \phi(Q)$.
   - $\phi(1) = 1$.

   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. - Hypothèse : I non réduit à 0.
     Il existe donc un polynôme P élément de $\mathbf{Q}[X]$, non nul tel que $P(a) = 0$. Notons d le degré de P et pour $i = 0, 1, \ldots, d$, a_i sont coefficient de degré i. Pour tout $i \in \{0, 1, \ldots, n\}$, a_i s'écrit $\frac{p_i}{q_i}$, avec $p_i \in \mathbf{Z}$ et $q_i \in \mathbf{N}^*$. Posons $\delta = q_0 \times q_1 \times \cdots \times q_d$. δP est un polynôme non nul à coefficients entiers et $(\delta P)(a) = 0$. Donc *a est algébrique.*
   - Hypothèse : a est algébrique.
     Donc a est racine d'un polynôme P non nul à coefficients entiers. Donc I admet P comme élément et *I est non réduit à* 0.
     Donc a est algèbrique si et seulement si I est non réduit à $\{0\}$.
6. I est un idéal de $\mathbf{Q}[X]$, donc, d'après le programme, il existe P élément de $\mathbf{Q}[X]$ (appelé générateur de I), tel que $I = P\mathbf{Q}[X]$, I étant non nul, $P \neq 0$. Soit $\tilde{P}$ un générateur de I. $\tilde{P} \in I$ donc $P | \tilde{P}$. par symétrie des rôles $\tilde{P} | P$ donc $\tilde{P}$ et P sont associés. Les générateurs de I sont associés, il en existe donc un et un seul unitaire, μ_a, qui est défini par $\mu_a = a^{-1}P$, avec a le coefficient dominant de P.

   $\mu_a(a) = 0$, donc μ_a ne saurait être un inversible de $\mathbf{Q}[X]$. Soient A et B des éléments de $\mathbf{Q}[X]$, tels que $\mu_a = AB$. $A(a)B(a) = \mu_a(a) = 0$. L'intégrité de $\mathbf{Q}$ assure donc que $A(a)$ ou $B(a)$ est nul. Prenons par exemple $A(a)$ nul. Alors $A \in I$ donc $\mu_a | A$, or $A | \mu_a$ donc A et μ_a sont associés et donc B est de degré 0. Donc μ_a est irréductible.

   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 $\mathrm{d}^\circ\mu_a = 1$. Il existe donc s et t rationels tels que $s \neq 0$ et $\mu_a = sX + t$. De $\mu_a(a) = 0$ on déduit $a = -\frac{t}{s}$, et donc $a \in \mathbf{Q}$. Par contaposition :
   si a est irrationnel, alors le degré de μ_a est supérieur ou égal à 2.

   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, étant à coefficients rationnels donc réels, il admet aussi comme racine $\overline{ia'} = -ia'$. Donc il existe $c \in \mathbf{R}^*$, tel que $A = c(X^2 - \frac{1-\sqrt{5}}{2})$. A étant à coefficients rationnels, c est rationnel, mais alors $c\frac{1-\sqrt{5}}{2}$ est rationnel ce qui conduit à la rationnalité de $\sqrt{5}$, ce qui est faux. Donc finalement un des polynômes A et B est de degré 0, et donc $X^4 - X^2 - 1$ est *irréductible*.
Donc μ_a, diviseur de $X^4 - X^2 - 1$ est associé à $X^4 - X^2 - 1$. Ces deux polynômes étant unitaires ils sont égaux :

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

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 $x = P(a)$. La division euclidienne de P par μ_a conduit à l'existence de Q et R éléments de $\mathbf{Q}[X]$ tels que : $P = Q\mu_a + R$ et $\mathrm{d}^\circ R < \mathrm{d}^\circ \mu_a$. D'où $x = P(a) = Q(a)\mu_a(a) + R(a) = R(a)$. x étant non nul, R est non nul, Donc μ_a ne saurait divisé R, polynôme dont le degré est inférieur au sien. Or μ_a est irréductible dans $\mathbf{Q}[X]$ (cf. 6.), donc R et μ_a sont premiers entres eux dans $\mathbf{Q}[X]$. Le lemme de Bezout affirme donc l'existence de deux éléments U et V de $\mathbf{Q}[X]$ tels que $UR + V\mu_a = 1$. En substituant a à l'indéterminé X, on obtient :

$$1 = U(a)R(a) + V(a)\mu_a(a) = U(a)x.$$

Donc $U(a) = x^{-1}$ et donc $x^{-1} \in \mathbf{Q}[a]$. 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. le corps $\mathbf{Q}(a)$ contenant 1 et a et étant stable par multiplication, il contient a^i, pour $i = 0, 1 \ldots, n$. Par ailleurs $c_i \in \mathbf{Q}(a)$ (cf. 1.). Donc le corps $\mathbf{Q}(a)$ étant stable par multiplication est addition, il contient $\sum_{i=0}^{n} c_i a^i = x$. Donc $\mathbf{Q}[a] \subset \mathbf{Q}(a)$.

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 $\mathbf{R}$. En raisonnant comme dans le début de la question on montre que tout élément x de $\mathbf{Q}[a]$ est de la forme $x = R(a)$ où R est un élément de $\mathbf{Q}[X]$, de degré inférieur strictement à n, degré de μ_a. En notant c_i le coefficient d'ordre i de R, pour $i = 0, 1, 2 \ldots, n-1$, x s'écrit :

$$x = \sum_{i=0}^{n-1} c_i a^i.$$

Donc $\mathbf{Q}[a] \subset \underset{\mathbf{Q}}{\mathrm{vect}}(a^0, a^1, \ldots, a^{n-1})$. L'inclusion inverse étant évidente,

$$Q[a] = \underset{\mathbf{Q}}{\mathrm{vect}}(a^0, a^1, \ldots, a^{n-1}).$$

la famille *la famille* $(a^0, a^1, \ldots, a^{n-1})$ *engendre donc* $\mathbf{Q}[a]$.

Montrons que la famille $(a^0, a^1, \ldots, a^{n-1})$ est libre. Soient $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ des rationnels tels que : $\lambda_0 a^0 + \lambda_1 a^1 + \cdots + \lambda_{n-1} a^{n-1} = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda_0 X^0 + \lambda_1 X^1 + \cdots + \lambda_{n-1} X^{n-1}$. Supposons C non nul. Alors par division euclidienne : $\mu_a = \tilde{Q}C + R$ avec $\tilde{Q} \in \mathbf{Q}[X]$, $R \in \mathbf{Q}[X]$ et $\mathrm{d}^\circ R \leq n - 1$. En substituant dans cette égalité a à l'indéterminée, il vient $0 = R(a)$. Donc $R(a)$ est

élément de I, il est donc divisible par μ_a, mais son degré étant inférieur strictement à celui de μ_a, c'est qu'il est nul. Donc C divise μ_a. Mais μ_a étant irréductible C est constant non nul, ce qui contredit $C(a) = 0$. Donc C est nul, c'est-à-dire : $\lambda_0 = \lambda_0 = \cdots = \lambda_{n-1} = 0$. D'où la liberté de $(a^0, a^1, \ldots, a^{n-1})$.

Finalement $(a^0, a^1, \ldots, a^{n-1})$ est une base de $\mathbf{Q}[a]$, 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 $\mathbf{Q}(a)$ est de dimension infinie.