DM 13 - Nombres algébriques, nombres transcendants

1 L'algèbre $\mathbb{Q}[\alpha]$

1. Soient $P, Q \in \mathbb{Q}[X]$, soient $\lambda, \mu \in \mathbb{Q}$. On a :

$$\phi_\alpha(\lambda P + \mu Q) = (\lambda P + \mu Q)(\alpha) = \lambda P(\alpha) + \mu Q(\alpha) = \lambda \phi_\alpha(P) + \mu \phi_\alpha(Q).$$

Donc ϕ_α est linéaire. De plus, $\phi_\alpha(1) = 1$ et $\phi_\alpha(PQ) = (PQ)(\alpha) = P(\alpha)Q(\alpha) = \phi_\alpha(P)\phi_\alpha(Q)$. Donc, ϕ_α est un morphisme d'anneaux. (*Pas besoin de montrer que ϕ_α préserve les lois $+$, ça a déjà été fait dans la linéarité.*)

2. Comme ϕ_α est un morphisme d'anneaux, son image $\mathbb{Q}[\alpha]$ est un sous-anneau de $\mathbb{C}$.

La famille $(X^n)_{n\in\mathbb{N}}$ est une famille génératrice de $\mathbb{Q}[X]$. Donc la famille $(\phi_\alpha(X^n))_{n\in\mathbb{N}} = (\alpha^n)_{n\in\mathbb{N}}$ est une famille génératrice de l'image de ϕ_α, c'est-à-dire de $\mathbb{Q}[\alpha]$. Autrement dit, $\mathbb{Q}[\alpha]$ est le $\mathbb{Q}$-espace vectoriel engendré par $\{\alpha^n, n \in \mathbb{N}\}$.

3. - On suppose $i)$. Par hypothèse, on peut trouver $\beta_1, \dots, \beta_n \in \mathbb{Q}[\alpha]$ qui forment une famille de générateurs de $\mathbb{Q}[\alpha]$. Chaque β_i est de la forme $P_i(\alpha)$, où $P_i \in \mathbb{Q}[X]$. En particulier, si on note $d-1$ le degré maximal des P_i, chaque β_i est combinaison linéaire des α^k, pour $k \in [\![0, d-1]\!]$. Ainsi, la famille $(\alpha^k)_{k\in[\![0,d-1]\!]}$ est génératrice de $\mathbb{Q}[\alpha]$. En particulier, $\alpha^d \in \text{Vect}\left(\alpha^k, k \in [\![0, d-1]\!]\right)$. Ce qui montre $ii)$.
   - On suppose $ii)$. On peut donc trouver $\lambda_0, \dots, \lambda_{d-1} \in \mathbb{Q}$ tels que $\alpha^d = \sum_{k=0}^{d-1} \lambda_k \alpha^k$. Notons $P = X^d - \sum_{k=0}^{d-1} \lambda_k X^k$. Alors, $P(\alpha) = 0$, ce qui revient à dire que $P \in \text{Ker}\,\phi_\alpha$. Donc ϕ_α n'est pas injectif et on a $iii)$.
   - On suppose $iii)$. Soit P un polynôme de degré $d \in \mathbb{N}$ dans $\text{Ker}\,\phi_\alpha$. Soit $n \in \mathbb{N}$. Écrivons la division euclidienne de X^n par P :

$$X^n = PQ + R,$$

avec $R \in \mathbb{Q}_{d-1}[X]$. En évaluant en α, on a $\alpha^n = P(\alpha)Q(\alpha) + R(\alpha) = R(\alpha)$. Or, $R(\alpha) \in \text{Vect}(\alpha^0, \dots, \alpha^{d-1})$. Donc, tout α^n est dans $\text{Vect}(\alpha^0, \dots, \alpha^{d-1})$. Commes les α^n (avec $n \in \mathbb{N}$) engendrent $\mathbb{Q}[\alpha]$, on en déduit que $\mathbb{Q}[\alpha] = \text{Vect}(\alpha^0, \dots, \alpha^{d-1})$. D'où $i)$.

4. Le noyau d'un morphisme d'anneaux quelconque est toujours un idéal. Montrons-le dans ce cas particulier.

   - $\text{Ker}\,\phi_a$ est un sous-groupe additif de $\mathbb{Q}[X]$ car ϕ_a est un morphisme d'anneaux, donc de groupes.
   - Soit $P \in \text{Ker}\,\phi_a$ et $Q \in \mathbb{Q}[X]$. Alors $\phi_a(PQ) = \phi_a(P)\phi_a(Q) = 0$ car $\phi_a(P) = 0$. Donc $PQ \in \text{Ker}\,\phi_a$, ce qui montre que $\text{Ker}\,\phi_a$ est un idéal de $\mathbb{Q}[X]$.

5. Soient $R, Q \in \mathbb{Q}[X]$ tels que $P_\alpha = RQ$. En évaluant en α, on a $R(\alpha)Q(\alpha) = 0$. Par intégrité de $\mathbb{C}$, l'un des deux facteurs est nul, disons $R(\alpha)$. Alors $R \in \operatorname{Ker}\phi_\alpha$, donc P_α divise R. Comme R divise P_α par hypothèse, ces deux polynômes sont associés.

   Donc P_α est irréductible dans $\mathbb{Q}[X]$.

6. Un nombre α est algébrique de degré 1 ssi il est racine d'un polynôme unitaire $P \in \mathbb{Q}[X]$ de degré 1. Un tel polynôme s'écrit $X - q$, où $q \in \mathbb{Q}$. On en déduit que les nombres algébriques de degré 1 sont les nombres rationnels.

7. Si α est algébrique de degré 2, alors α est racine de P_α, qui est unitaire, à coefficients rationnels, de degré 2 et irréductible dans $\mathbb{Q}[X]$. Réciproquement, si un nombre α est racine d'un polynôme $P \in \mathbb{Q}[X]$, unitaire, de degré 2 et irréductible, alors il est algébrique de degré 2. En effet, comme il est annulé par un polynôme de degré 2, il est algébrique de degré 1 ou 2. Mais s'il était de degré 1, il serait rationnel, ce qui contredirait l'irréductibilité de P.

   Il reste à comprendre quand un polynôme $P \in \mathbb{Q}[X]$ de degré 2, unitaire est irréductible dans $\mathbb{Q}[X]$. Un tel polynôme s'écrit $P = X^2 + mx + p$. Il est irréductible ssi il n'a pas de racines dans $\mathbb{Q}$ (car de degré 2). Or, si $\delta \in \mathbb{C}$ est tel que $\delta^2 = m^2 - 4p$, les racines sont données par $-m \pm \delta$. Ces racines sont rationnelles ssi δ l'est ssi le discriminant est le carré d'un nombre rationnel. Ceci conclut.

8. (a) Si $\gamma \in \mathbb{Q}[\alpha]$, alors $m_\beta(\gamma) = \beta\gamma \in \mathbb{Q}[\alpha]$ car $\mathbb{Q}[\alpha]$ est un sous-anneau de $\mathbb{C}$. Ainsi, m_β induit un endomorphisme de $\mathbb{Q}[\alpha]$.

   Si γ est dans le noyau de cet endomorphisme, alors $\beta\gamma = 0$ et donc $\gamma = 0$ par intégrité de $\mathbb{C}$ (et parce que $\beta \neq 0$). Donc cet endomorphisme est injectif.

   Pour la surjectivité, deux possibilités :
   - Comme on est en dimension finie, il y a équivalence pour un endomorphisme à être injectif ou surjectif.
   - On peut aussi donner un argument direct. Comme β est dans $\mathbb{Q}[\alpha]$, il s'écrit $Q(\alpha)$ pour un $Q \in \mathbb{Q}[X]$. Comme β est non nul, P_α ne divise pas Q, et comme P_α est irréductible, il est premier avec Q. On peut donc trouver une relation de Bézout du type : $UP_\alpha + VQ = 1$, avec $U, V \in \mathbb{Q}[X]$. En évaluant en α, on obtient : $V(\alpha)Q(\alpha) = 1$ et donc, $\beta = Q(\alpha)$ admet un inverse dans $\mathbb{Q}[\alpha]$. En notant β^{-1} cet inverse, on a $y = m_\beta(\beta^{-1}y)$, pour tout $y \in \mathbb{Q}[\alpha]$, et donc m_β est surjective.

   (b) Ainsi, dans l'anneau $\mathbb{Q}[\alpha]$, tout élément non nul a un inverse. Donc, $\mathbb{Q}[\alpha]$ est un corps.

9. On raisonne par contraposée. Si α est transcendant, le morphisme $\phi_\alpha : \mathbb{Q}[X] \to \mathbb{C}$ est injectif. C'est donc un isomorphisme de $\mathbb{Q}[X]$ vers $\mathbb{Q}[\alpha]$ (qui est l'image de ϕ_α). Or, $\mathbb{Q}[X]$ n'est pas un corps (seuls les polynômes constants non nuls sont inversibles) ; donc $\mathbb{Q}[\alpha]$ qui lui est isomorphe (en tant qu'anneau) n'est pas non plus un corps.

2 Le corps $\overline{\mathbb{Q}}$ des nombres algébriques

10. (a) En reprenant la démonstration de $iii) \implies i)$ dans la question 3., on montre que $\mathbb{Q}[\alpha] = \operatorname{Vect}(\alpha^0, \ldots, \alpha^{d-1})$ et $\mathbb{Q}[\beta] = \operatorname{Vect}(\beta^0, \ldots, \beta^{d'-1})$. Donc, si $(k, \ell) \in \mathbb{N}^2$, on peut

trouver $\lambda_0, \dots, \lambda_{d-1}$ et $\mu_0, \dots, \mu_{d'-1}$ tels que $\alpha^k = \sum_{i=0}^{d-1} \lambda_i \alpha^i$ et $\beta^\ell = \sum_{j=0}^{d'-1} \mu_j \beta^j$. Alors,

$$\alpha^k \beta^\ell = \sum_{\substack{0 \le i \le d-1 \\ 0 \le j \le d'-1}} \lambda_i \mu_j \alpha^i \beta^j.$$

Ceci montre que chaque $\alpha^k \beta^\ell$ est dans $\mathrm{Vect}\left(\alpha^k \beta^\ell, (k,\ell) \in \mathbb{N}^2\right)$. Donc,

$$\mathbb{Q}[\alpha, \beta] = \mathrm{Vect}\left(\alpha^k \beta^\ell, (k,\ell) \in \mathbb{N}^2\right).$$

(b) On a $\mathbb{Q}[\alpha+\beta] \subset \mathbb{Q}[\alpha, \beta]$. En effet, par la formule du binôme de Newton,

$$\forall n \in \mathbb{N}, (\alpha+\beta)^n = \sum_{k=0}^{n} \binom{n}{k} \alpha^k \beta^{n-k},$$

ce qui montre que les puissances de $\alpha+\beta$ sont des combinaisons linéaires à coefficients dans $\mathbb{Q}$ de produits $\alpha^i \beta^j$.
D'après la question précédente, $\mathbb{Q}[\alpha, \beta]$ est de dimension finie, donc $\mathbb{Q}[\alpha+\beta]$, qui en est un sous-espace vectoriel, aussi. Donc, $\alpha+\beta$ est algébrique.

L'argument pour $\alpha\beta$ est analogue (et même plus simple).

11. La question précédente montre que $\overline{\mathbb{Q}}$ est un sous-anneau de $\mathbb{C}$ (puisque 1 est bien sûr algébrique). De plus, on a montré en première partie que si $\alpha \neq 0$ est algébrique, alors $\mathbb{Q}[\alpha]$ est un corps. Ceci implique que $\alpha^{-1} \in \mathbb{Q}[\alpha]$. Donc, que $\mathbb{Q}[\alpha^{-1}] \subset \mathbb{Q}[\alpha]$ (*Il y a en fait égalité*) Donc, $\mathbb{Q}[\alpha^{-1}]$ est de dimension finie ce qui implique que α^{-1} est aussi dans $\overline{\mathbb{Q}}$.

Donc, $\overline{\mathbb{Q}}$ est un corps.

12. Soit $\alpha \in \mathbb{C}$, soit $n \in \mathbb{N}^*$ tels que $\alpha^n \in \overline{\mathbb{Q}}$. On considère P_{α^n} le polynôme minimal de α^n. On a donc :

$$P_{\alpha^n}(\alpha^n) = 0.$$

Cette égalité montre que α est racine du polynôme $P(X^n) \in \mathbb{Q}[X]$. Donc, $\alpha \in \overline{\mathbb{Q}}$.

3 Mesure d'irrationalité et constante de Liouville

13. Soit x un réel, soit $\mu < 1$. Fixons $A > 0$. On cherche à montrer qu'il existe un couple $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $x \neq \frac{p}{q}$ et $\left|x - \frac{p}{q}\right| < \frac{A}{q^\mu}$. Pour $q \in \mathbb{N}^*$ donné, on considère la fraction $\frac{p}{q}$ la plus proche (mais distincte) de x. On a donc $|x - \frac{p}{q}| \le \frac{1}{q}$. Or, si q est suffisamment grand, $\frac{1}{q} < \frac{A}{q^\mu}$, car $\mu < 1$. On peut donc bien trouver un tel couple (p,q). Ceci montre qu'aucun $\mu < 1$ n'est dans l'ensemble $\mathscr{A}_x$, donc $\mu(x) \ge 1$.

Soit $x = \frac{a}{b}$ un rationnel. Si $\frac{p}{q}$ est un rationnel distinct de x, on a (on suppose $b, q > 0$)

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} \ge \frac{1}{bq},$$

car $aq - bp \neq 0$.

Ceci montre que, $1 \in \mathscr{A}_x$ (en prenant $A = \dfrac{1}{b}$. Donc $\mu(x) = 1$ si $x \in \mathbb{Q}$.

14. (a) Le polynôme minimal P_x de x est de degré d et à coefficients rationnels, ayant x comme racine. En le multipliant par le ppcm des dénominateurs de ses coefficients, on définit un polynôme P à coefficients entiers, de degré d tel que $P(x) = 0$. Enfin, P n'a pas de racine rationnelle. En effet, si P avait une racine rationnelle, alors P_x aussi. Donc P_x ne serait pas irréductible, en contradiction avec la question 5.

    (b) Notons $M = \sup_{t \in [x-1 x+1]} |P'(t)|$, bien défini par le théorème des bornes atteintes, appliquée à la fonction (continue) associée à P'. Par l'inégalité des accroissements finis, on a

$$\left|P\left(\frac{p}{q}\right)\right| = \left|P\left(\frac{p}{q}\right) - P(x)\right| \leq M\left|x - \frac{p}{q}\right|.$$

    (c) Notons $P = \sum_{k=0}^{d} a_k X^k$, avec pour tout k, $a_k \in \mathbb{Z}$. Alors $q^d P\left(\dfrac{p}{q}\right) = \sum_{k=0}^{d} a_d p^k q^{d-k} \in \mathbb{Z}$. De plus, cette quantité est non nulle, car sinon $\dfrac{p}{q}$ serait racine de P. Ceci montre le premier point.

    On en déduit que $\left|q^d P\left(\dfrac{p}{q}\right)\right| \geq 1$. Avec l'inégalité obtenue à la question précédente, on obtient :

$$\left|x - \frac{p}{q}\right| \geq \frac{1}{Mq^d}.$$

    (d) L'inégalité précédente a été obtenue sous l'hypothèse $\dfrac{p}{q} \in [x-1, x+1]$. Mais si cette hypothèse n'est pas vérifiée, alors $\left|x - \dfrac{p}{q}\right| > 1 \geq \dfrac{1}{q^d}$. Ainsi, en notant $A = \min(1, \dfrac{1}{M})$, on a dans tous les cas :

$$\left|x - \frac{p}{q}\right| \geq \frac{A}{q^d}.$$

    Ceci montre que $d \in \mathscr{A}_x$, donc que $\mu(x) \leq d$.

15. On suppose que x est un nombre de Liouville. En particulier, il est irrationnel. Soit $d \in \mathbb{R}$. Comme la mesure d'irrationalité de x est $+\infty$, on a :

$$\forall A > 0, \exists (p,q) \in \mathbb{Z} \times \mathbb{N}^* : 0 < |x - \frac{p}{q}| < \frac{A}{q^d}.$$

Donc, pour tout $n \in \mathbb{N}^*$, on peut trouver $(p_n, q_n) \in \mathbb{Z} \times \mathbb{N}^*$ tels que

$$0 < |x - \frac{p_n}{q_n}| < \frac{1}{nq^d} \leq \frac{1}{q^d}.$$

Le nombre de tels couples (p_n, q_n) est nécessairement infini (car les $|x - \dfrac{p_n}{q_n}|$ sont non nuls mais que $\dfrac{1}{nq^d}$ est arbitrairement petit quand n tend vers $+\infty$). Ceci montre le sens direct.

On suppose maintenant que x n'est pas un nombre de Liouville. On note $\mu \in [1, +\infty[$ un élément de $\mathscr{A}_x$. On fixe un $A > 0$ tel que

$$\forall (p,q) \in \mathbb{Z} \times \mathbb{N}^*, x \neq \frac{p}{q} \implies |x - \frac{p}{q}| \geq \frac{A}{q^\mu}.$$

Fixons maintenant un réel $d > \mu$. Si $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ est tel que $0 < |x - \frac{p}{q}| < \frac{1}{q^d}$, on a en particulier $x \neq \frac{p}{q}$ et $\frac{A}{q^\mu} < \frac{1}{q^d}$. Comme $d > \mu$, seul un nombre fini de q peut vérifier cette inégalité. De plus, pour chacune des valeurs possibles de q, l'inégalité $|x - \frac{p}{q}| < \frac{1}{q^d}$ ne peut être satisfaite que par un nombre fini de p.
Ainsi, seul un nombre fini de couples $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ peuvent vérifier $0 < |x - \frac{p}{q}| < \frac{1}{q^d}$. Ce qui conclut la réciproque.

16. Le sens direct est immédiat. Si $n \in \mathbb{N}$, on pose $d = n$ et on utilise la question précédente pour construire un couple (p_n, q_n) (on dispose d'une infinité de tels couples).
Pour la réciproque, on fixe $d \in \mathbb{R}$. Pour tout $n \geq d$, on peut construire un couple $(p_n, q_n) \in \mathbb{Z} \times [\![2, +\infty[$ tel que $|x - \frac{p_n}{q_n}| < \frac{1}{q_n^n} \leq \frac{1}{q_n^d}$. Il y a nécessairement une infinité de tels couples (p_n, q_n). En effet, sinon l'ensemble des valeurs de $|x - \frac{p_n}{q_n}|$ serait minoré par une constante strictement positive ; alors que la suite $\frac{1}{q_n^n}$ tend vers 0 (car $q_n \geq 2$). Ceci conclut.

17. La suite $\left(\sum_{k=0}^{n} \frac{1}{10^{k!}}\right)$ est croissante. De plus, pour tout $k \in \mathbb{N}, k! \geq k$, donc $\frac{1}{10^{k!}} \leq \frac{1}{10^k}$. Ceci montre que pour tout n :

$$\sum_{k=0}^{n} \frac{1}{10^{k!}} \leq \sum_{k=0}^{n} \frac{1}{10^k} < \frac{10}{9}.$$

Donc, la suite $\left(\sum_{k=0}^{n} \frac{1}{10^{k!}}\right)$ est majorée. Par le théorème de la limite monotone, elle est convergente. Donc, $\mathscr{L}$ est bien définie.

Soit $n \in \mathbb{N}$. On écrit $\sum_{k=0}^{n} \frac{1}{10^{k!}}$ sous la forme $\frac{p_n}{q_n}$ avec $q_n = 10^{n!}$. Alors,

$$\mathscr{L} - \frac{p_n}{q_n} = \sum_{k=n+1}^{+\infty} \frac{1}{10^{k!}} < \sum_{\ell=(n+1)!}^{+\infty} \frac{1}{10^\ell} = \frac{1}{10^{(n+1)!}} \frac{10}{9} < \frac{1}{10^{(n+1)!-1}}.$$

On constate aisément que $(n+1)! - 1 \geq n! \times n$. On en déduit que

$$\left|\mathscr{L} - \frac{p_n}{q_n}\right| = \mathscr{L} - \frac{p_n}{q_n} < \frac{1}{(10^{n!})^n} = \frac{1}{q_n^n}.$$

Ceci montre que $\mathscr{L}$ est un nombre de Liouville, donc $\mathscr{L}$ est transcendant.