I. Nombres algébriques

1) Supposons α algébrique. Alors il existe un polynôme non nul $P = a_0 + a_1 X + \cdots + a_p X^p \in \mathbb{Q}[X]$ tel que $a_0 + a_1\alpha + \cdots + a_p\alpha^p = 0$. Puisque P est non nul, la famille $(1, \alpha, \ldots, \alpha^p)$ est liée. Réciproquement, supposons que $(1, \alpha, \ldots, \alpha^p)$ est liée. Alors il existe $a_0, a_1, \ldots, a_p \in \mathbb{Q}$ non tous nuls tels que $a_0 + a_1\alpha + \cdots + a_p\alpha^p = 0$. En posant $P = a_0 + a_1 X + \cdots + a_p X^p \in \mathbb{Q}[X]$, on voit que α est algébrique.

2) Montrons que les nombres algébriques de degré 1 sont exactement les nombres rationnels. Si α est rationnel, alors α est racine de $X - \alpha \in \mathbb{Q}[X]$. Réciproquement, si α est algébrique de degré 1, il est racine de $a_1 X + a_0$ où $a_0, a_1 \in \mathbb{Q}$ et $a_1 \neq 0$. Donc $\alpha = -a_0/a_1 \in \mathbb{Q}$.

3) Le nombre complexe $\sqrt{3}$ est racine de $X^2 - 3$, donc est algébrique de degré $\leqslant 2$. Il n'est pas de degré 1 car sinon il serait rationnel d'après la question précédente.

4) Le nombre complexe i est racine de $X^2 + 1$, donc est algébrique de degré $\leqslant 2$. Il n'est pas rationnel, donc n'est pas de degré 1. Donc i est de degré 2.

5) Supposons α algébrique de degré 2. Alors α est racine de $a_0 + a_1 X + a_2 X^2$, et donc est aussi racine de $p + mX + X^2$ si $p = a_0/a_2$ et $m = a_1/a_2$. De plus, Δ n'est pas le carré d'un nombre rationnel, car sinon $\Delta = r^2$, où $r \in \mathbb{Q}$, et alors $\alpha = \dfrac{-m + |r|}{2}$ ou $\dfrac{-m - |r|}{2}$, et α serait rationnel. Donc α serait de degré 1.

Réciproquement, supposons α racine de $P = X^2 + mX + p$ dont le discriminant Δ n'est pas le carré d'un rationnel. Alors il existe un nombre complexe $r \in \mathbb{C} \setminus \mathbb{Q}$ tel que $\Delta = r^2$, et les racines de P sont alors $\dfrac{-m + r}{2}$ et $\dfrac{-m - r}{2}$. Ces nombres ne sont pas rationnels, sinon r le serait.

II. Sous-corps de $\mathbb{C}$

6) Vérifions que I_α est un idéal de $\mathbb{Q}[X]$. On a immédiatement que I_α est un sous-espace vectoriel, car contient le polynôme nul et est stable par combinaison linéaire. Puisque I_α n'est pas réduit à $\{0\}$, il existe d'après le cours un unique polynôme $M_\alpha \in \mathbb{Q}[X]$ unitaire ou nul tel que $I_\alpha = M_\alpha \mathbb{Q}[X]$.

7) Soit $q = \deg M_\alpha$. (En fait, c'est p.) Puisque la famille $(1, \alpha, \ldots, \alpha^{d-1})$ est liée, il existe $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{Q}[x]$ non nul tel que $P(\alpha) = 0$. Mais alors M_α divise P. Donc $q \leqslant d$.

Réciproquement, montrons par l'absurde que $d \leqslant q$. Sinon, $q < d$. Donc $M_\alpha = \sum_{k=0}^{q} a_k X^k$ annule α. Donc la famille $(1, \alpha, \ldots, \alpha^q)$ est liée, et est une sous-famille de $(1, \alpha, \ldots, \alpha^{d-1})$ qui est libre. Absurde.

8) On écrit $M_\alpha = PQ$ avec $P, Q \in \mathbb{Q}[X]$. Par symétrie, on peut supposer que α est racine de P. Par minimalité de d, $\deg P \geqslant p = \deg M_\alpha$. Donc $\deg Q = 0$ et M_α est irréductible sur $\mathbb{Q}$.

9) Puisque $M'_\alpha \in \mathbb{Q}[X]$ est non nul et de degré strictement inférieur à celui de M_α, le polynôme M_α ne divise pas M'_α. Donc $M'_\alpha \notin I_\alpha$, *i.e.* $M'_\alpha(\alpha) \neq 0$. D'après le cours, M_α n'admet pas de racines multiples.

10) Exemple 1. Le polynôme $X^3 - 5$ est de degré 3 et n'admet pas de racine dans $\mathbb{Q}$: en effet, si $r = p/q$ est racine, avec $p, q \in \mathbb{N}^*$, alors $p^3 = 5q^3$. Si r est l'exposant de 5 dans p et s celui de 5 dans q, alors $3p = 3s + 1$, ce qui est absurde.

On en déduit, d'après le cours, que $X^3 - 5$ est irréductible sur $\mathbb{Q}$. Mais alors, α est algébrique de degré $\deg(X^3 - 5) = 3$.

11) Exemple 2. On étudie sur $\mathbb{R}$ la fonction $t \mapsto P(t)$. On a $P'(t) = 3t^2 + 1 > 0$, donc la fonction polynomiale P est strictement croissante. Puisque $\lim_{t \to -\infty} P(t) = -\infty$ et $\lim_{t \to +\infty} P(t) = +\infty$, P admet une racine d'après le théorème des valeurs intermédiaires. Par stricte monotonie, cette racine réelle est unique.

Montrons par l'absurde que cette racine n'est pas rationnelle. Sinon, soient $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux tels que $\dfrac{p^3}{q^3} + \dfrac{p}{q} + 1 = 0$. On a alors $p^3 + pq^2 + q^3 = 0$. Puisque q divise $pq^2 + q^3$, q divise p^3. Puisque p et q sont premiers entre eux, q divise 1 d'après le lemme de Gauss. Donc $q = \pm 1$, et donc $q = 1$. De même, p divise q^3 et donc divise q, d'où $p = \pm 1$. Puisque $p/q < 0$, on a $p = -1$. Or -1 n'est pas racine de $X^3 + X + 1$. Donc $X^3 + X + 1$ n'admet pas de racine rationnelle.

Pour exprimer l'inverse de $1 + \alpha$, on dispose de deux méthodes. Soit on résout le système obtenu à partir de $(1+\alpha)(a_0 + a_1\alpha + a_2\alpha^2) = 1$, ce qui conduit

(en utilisant $\alpha^3 = -1-\alpha$) au système

$$\left\{\begin{array}{rcl} a_0 - a_2 & = & 1 \\ a_0 + a_1 - a_2 & = & 0 \\ a_2 + a_1 & = & 0, \end{array}\right.$$

d'où $a_0 = 2$, $a_1 = -1$ et $a_2 = 1$. Soit on utilise le polynôme minimal $X^3 + X + 1$ de α. L'algorithme d'Euclide étendu donne – en une seule division – $X^3 + X + 1 = (X+1)(X^2 - X + 2) - 1$. En évaluant en α, on obtient encore $1 = (\alpha+1)(\alpha^2 - \alpha + 2)$.

III. Polynôme minimal

12) Par définition $\mathbb{Q}[\alpha]$, la famille est génératrice. Elle est libre par définition de d.

13) On pouvait vérifier les axiomes un à un. On préfère ici une preuve plus conceptuelle. On va montrer que l'application $F : \mathbb{Q}[X] \to \mathbb{C}$, $P \mapsto P(\alpha)$ est un morphisme d'algèbre. Son image est alors une sous-algèbre de $\mathbb{C}$, dont on vérifiera que c'est $\mathbb{Q}[\alpha]$.

On a immédiatement F linéaire et $F(PQ) = (PQ)(\alpha) = P(\alpha)Q(\alpha)$. De plus $F(1) = 1$. Donc F est un morphisme d'algèbre. Montrons que $\mathrm{Im}\, F = \mathbb{Q}[\alpha]$. On a déjà $\mathrm{Im}\, F \supset \mathbb{Q}[\alpha]$ car si $P = X^k$, $F(X^k) = a^k \in \mathrm{Im}\, F$ pour tout $0 \leqslant k \leqslant d-1$. Réciproquement, si $z \in \mathrm{Im}\, F$, alors $z = P(\alpha)$. On écrit la division euclidienne de P par M_α : $P = M_\alpha Q + R$ où $\deg R < d$. Mais alors $z = P(\alpha) = M_\alpha(\alpha)Q(\alpha) + R(\alpha) = R(\alpha) \in \mathbb{Q}[\alpha]$ car $degR < d$.

14) Puisque $\mathbb{Q}[\alpha]$ est une algèbre, $\beta z \in \mathbb{Q}[\alpha]$ dès que $\beta, z \in \mathbb{Q}[\alpha]$. Donc f_β est bien définie. Elle est linéaire (évident), et $z \in \ker f_\beta$ si et seulement si $\beta z = 0$. Donc $z = 0$. Puisque le noyau est réduit à 0, f_β est injective. Puisque $\mathbb{Q}[\alpha]$ est de dimension finie (égale à d), f_β est un automorphisme.

15) Puisque $\mathbb{Q}[\alpha]$ est une sous-algèbre de $\mathbb{C}$, il suffit de démontrer que tout élément non nul de $\mathbb{Q}[\alpha]$ admet un inverse dans $\mathbb{Q}[\alpha]$. Soit $\beta \in \mathbb{Q}[\alpha]$ non nul. Alors 1 admet un antécédent α' dans $\mathbb{Q}[\alpha]$ par f_α. Cet antécédent vérifie $\alpha\alpha' = 1$, et donc $\alpha' = \alpha^{-1}$.

IV. Cloture algébrique de $\mathbb{Q}$

16) Montrons que la famille $(\alpha^k\beta^n)_{0\leqslant k\leqslant p-1, 0\leqslant n\leqslant q-1}$ est une partie génératrice de $\mathbb{Q}[\alpha,\beta]$. Puisque $\alpha^k \in \mathbb{Q}[\alpha]$, α^k est une combinaison linéaire de $1, \alpha, \ldots, \alpha^{p-1}$. De même β^n est un combinaison linéaire de $1, \beta, \ldots, \beta^{q-1}$. En développant $\alpha^k\beta^n$, on trouve une combinaison linéaire des $\alpha^k\beta^n$ avec $0 \leqslant k \leqslant p-1$ et $0 \leqslant n \leqslant q-1$.

17) Déjà $\mathbb{Q}[\alpha,\beta]$ est un espace vectoriel car c'est le sous-espace vectoriel engendrée par une partie. De plus $1 \in \mathbb{Q}[\alpha,\beta]$.

Soient $z, z' \in \mathbb{Q}[\alpha,\beta]$. Alors $z = \sum_{0\leqslant i,j\leqslant N} \lambda_{i,j}\alpha^i\beta^j$ et $z' = \sum_{0\leqslant r,s\leqslant N} \mu_{r,s}\alpha^r\beta^s$, avec $N \in \mathbb{N}$ et $\lambda_{i,j}, \mu_{r,s} \in \mathbb{Q}$. Donc $zz' = \sum_{0\leqslant i,j,r,s\leqslant N} \lambda_{i,j}\mu_{r,s}\alpha^{i+r}\beta^{j+s} \in \mathbb{Q}[\alpha,\beta]$. Donc $\mathbb{Q}[\alpha,\beta]$ est stable par produit. Donc $\mathbb{Q}[\alpha,\beta]$ est une sous-algèbre de $\mathbb{C}$.

18) Soit $\gamma \in \mathbb{Q}[\alpha,\beta]$. Il s'agit de démontrer qu'il existe $d \in \mathbb{N}^*$ tel que $(1, \gamma, \ldots, \gamma^d)$ est liée. Or si $d \geqslant pq$, alors cette famille compte $pq+1$ éléments et $\dim \mathbb{Q}[\alpha,\beta] \leqslant pq$ d'après la question 16. Donc cette famille est liée, et γ est donc algébrique.

19) Il suffit de démontrer que tout $\gamma \in \mathbb{Q}[\alpha,\beta]$ non nul admet un inverse dans $\mathbb{Q}[\alpha,\beta]$. Soit $f_\gamma : \mathbb{Q}[\alpha,\beta] \to \mathbb{Q}[\alpha,\beta]$ la multiplication par γ. Cette application est bien définie car $\mathbb{Q}[\alpha,\beta]$ est une algèbre. Elle est injective car $\gamma z = 0$ implique $z = 0$. Puisque $\mathbb{Q}[\alpha,\beta]$ est de dimension finie, f_γ est aussi surjective. Donc 1 a un antécédent par f_γ, et cet antécédent est l'inverse de γ.

20) Déjà $(\overline{\mathbb{Q}}, +)$ est un sous-groupe de $\mathbb{C}$ car c'est un sous-espace vectoriel. En effet, si $\alpha, \beta \in \overline{\mathbb{Q}}$ et $\lambda, \mu \in \mathbb{Q}$, alors $\lambda\alpha + \mu\beta \in \mathbb{Q}[\alpha,\beta] \subset \overline{\mathbb{Q}}$. C'est même une sous-algèbre de $\mathbb{C}$ car $\alpha\beta \in \mathbb{Q}[\alpha,\beta] \subset \overline{\mathbb{Q}}$.

Il reste à montrer que tout $\alpha \in \overline{\mathbb{Q}}$ non nul admet un inverse dans $\overline{\mathbb{Q}}$. Or l'inverse de α appartient à $\mathbb{Q}[\alpha] = \mathbb{Q}[\alpha,\alpha]$ qui est inclus dans $\overline{\mathbb{Q}}$. Donc $\overline{\mathbb{Q}}$ est un corps.

21) Soit $P \in \overline{\mathbb{Q}}[X]$ non nul et $z \in \mathbb{C}$ une racine de P. Quitte à diviser par le coefficient dominant – ce qui ne change pas les racines – on peut supposer P unitaire. On écrit $P = X^n + \sum_{k=0}^{n-1} a_k X^k$ où $a_k \in \overline{\mathbb{Q}}$. Soit d_k le degré du nombre algébrique a_k. Soit $\mathbb{L} = \mathrm{Vect}\{a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} z^p \mid 0 \leqslant m_k \leqslant d_k - 1 \text{ et } 0 \leqslant p \leqslant n-1\}$.

Montrons d'abord que $z^p \in \mathbb{L}$ pour tout $p \in \mathbb{N}$. C'est vrai par définition pour $0 \leqslant p \leqslant n-1$. C'est vrai pour n car $z^n = -a_0 - a_1 z \cdots - a_{n-1} z^{n-1} \in \mathbb{L}$. Par récurrence sur p. Supposons la propriété vraie pour $p \geqslant n$. Alors $z^{p+1} = z^{p+1-n}(-a_0 - a_1 z \cdots - a_{n-1} z^{n-1})$ et par hypothèse de récurrence, il s'agit d'une somme d'éléments de $\mathbb{L}$ (car $\mathbb{L}$ est stable par multiplication par les a_k).

Puisque $\mathbb{L}$ est de dimension finie et contient $\mathbb{Q}[z]$, alors $\mathbb{Q}[z]$ est de dimension finie et z est algébrique.

V. Transcendance de e

22) Montrons par récurrence sur k que pour tout $k \in \mathbb{N}$, on a

$$I(t) = e^t \sum_{i=0}^{k} P^{(i)}(0) - \sum_{i=0}^{k} P^{(i)}(t) + e^t \int_0^t e^{-u} P^{(k+1)}(u)\,du.$$

Initialisation : on intègre par parties en posant $f'(u) = e^{-u}$ et $g(u) = P(u)$. On a ainsi

$$\begin{aligned} I(t) &= e^t \left[-e^{-u}P(u)\right]_{u=0}^{u=t} + e^t \int_0^t e^{-u} P'(u)\,du \\ &= e^t P(0) - P(t) + e^t \int_0^t e^{-u} P'(u)\,du. \end{aligned}$$

Hérédité : Supposons la propriété vraie pour un entier naturel k. On a donc

$$I(t) = e^t \sum_{i=0}^{k} P^{(i)}(0) - \sum_{i=0}^{k} P^{(i)}(t) + e^t \int_0^t e^{-u} P^{(k+1)}(u)\,du.$$

On intègre par parties $e^t \displaystyle\int_0^t e^{-u} P^{(k+1)}(u)\,du$, ce qui donne

$$e^t \int_0^t e^{-u} P^{(k+1)}(u)\,du = e^t \left[-e^{-u} P^{(k+1)}(u)\right]_{u=0}^{u=t} + e^t \int_0^t e^{-u} P^{(k+2)}(u)\,du$$

et donc

$$\begin{aligned} I(t) &= e^t \sum_{i=0}^{k} P^{(i)}(0) - \sum_{i=0}^{k} P^{(i)}(t) - P^{(k+1)}(t) + e^t P^{(k+1)}(0) \\ &\quad + e^t \int_0^t e^{-u} P^{(k+2)}(u)\,du \\ &= e^t \sum_{i=0}^{k+1} P^{(i)}(0) - \sum_{i=0}^{k+1} P^{(i)}(t) + e^t \int_0^t e^{-u} P^{(k+2)}(u)\,du. \end{aligned}$$

Pour $k \geqslant \deg P + 1$, on a la formule demandée puisqu'alors $P^{(k)} = 0$.

23) On a

$$\begin{aligned} J &= \sum_{k=0}^{n} \left(a_k e^k \sum_{i=0}^{q} P^{(i)}(0) - a_k \sum_{i=0}^{q} P^{(i)}(k) \right) \\ &= \underbrace{\left(\sum_{k=0}^{n} a_k e^k \right)}_{=0} \left(\sum_{i=0}^{q} P^{(i)}(0) \right) - \sum_{k=0}^{n} \sum_{i=0}^{q} a_k P^{(i)}(k). \end{aligned}$$

Puisque $P \in \mathbb{Z}[X]$, $P^{(i)}(k) \in \mathbb{Z}$ et J est un entier.

Montrons que $(p-1)!$ divise $P^{(i)}(0)$ pour tout entier i. Si $i < p-1$, alors $P^{(i)}(0) = 0$ car 0 est racine d'ordre $p-1$ de P. Si $i \geqslant p-1$, on écrit $P = X^{p-1}A$ où $A \in \mathbb{Z}[X]$. D'après la formule de Leibniz,

$$P^{(i)} = \sum_{r=0}^{i} \binom{i}{r} \left(X^{p-1}\right)^{(r)} A^{(i-r)}.$$

En évaluant en 0, il ne reste que

$$P^{(i)}(0) = \binom{i}{p-1} (p-1)! A^{(i-p+1)}(0)$$

car $\left(X^{p-1}\right)^{(r)}(0)$ est nul si $r \neq p-1$ et vaut $(p-1)!$ si $r = p-1$. Puisque $A \in \mathbb{Z}[X]$, alors $A^{(i-p+1)}$ aussi et donc $A^{(i-p+1)}(0) \in \mathbb{Z}$. Donc $(p-1)!$ divise $P^{(i)}(0)$.

Montrons que $p!$ divise $P^{(i)}(k)$ lorsque $k \in [\![1, n]\!]$. On écrit $P = (X-k)^p B_k$. Comme précédemment, d'après la formule de Leibniz et en évaluant en k,

on obtient

$$P^{(i)}(k) = \binom{i}{p} p! B_p^{(i-p)}(k).$$

Puisque $B_p \in \mathbb{Z}[X]$, $p!$ divise $P^{(i)}(k)$. *A fortiori*, $(p-1)!$ divise tous les $P^{(i)}(k)$, donc aussi J.

Montrons que pour p premier assez grand, J est non nul. Déjà,

$$\begin{aligned} J &\equiv -\sum_{k=0}^{n}\sum_{i=0}^{q} a_k P^{(i)}(0) \mod p! \\ &\equiv -a_0 \sum_{i=0}^{q} a_k P^{(i)}(0) \mod p!. \end{aligned}$$

Or $P = X^{p-1}A_0^p$ où $A_0 \in \mathbb{Z}[X]$. On a vu que

$$P^{(i)}(0) = (p-1)!\binom{p-1}{i}\left(A_0^p\right)^{(i-p+1)}(0).$$

Si $i \geqslant p$, on a donc $(A_0)^{(i-p+1)}(0) = p\left(A_0' A_0^p\right)^{(i-p)}(0)$, et ainsi $p!$ divise $P^{(i)}(0)$. Si $i < p-1$, $P^{(i)}(0) = 0$, comme on l'a déjà prouvé. Donc $J \equiv -a_0 P^{(p-1)}(0) \mod p!$. Or,

$$\begin{aligned} a_0 P^{(p-1)}(0) &= a_0(p-1)!\binom{p-1}{p-1} A_0^p(0) \\ &= a_0(p-1)!(-1)^p(-2)^p\cdots(-n)^p \\ &= a_0(p-1)!(-1)^n p(n!)^p. \end{aligned}$$

Si p est premier et strictement supérieur à n et a_0 (il en existe puisque l'ensemble des nombres premiers est infini), il ne divise pas $a_0 P^{(p-1)}(0)$, et donc pas J non plus, et ainsi J est non nul.

24) On majore $|J|$. On a $|J| \leqslant \sum_{k=0}^{n} |a_k| e^k \int_0^k e^{-u}|P(u)|du$. Soit $a = \max|a_k|$. Alors $|J| \leqslant ae^n(n+1)\int_0^n |P(u)|du$, car $e^{-u} \leqslant 1$ sur $[0,n]$ et $|P(u)| \geqslant 0$. De plus, $|P(u)| = |u|^{p-1}|u-1|^p\cdots|u-n|^p \leqslant n^{p-1}(n^n)^p$. D'où $|J| \leqslant ae^n(n+1)nn^{p-1}(n^n)^p$. Quitte à changer a en $\max(1,a)$, on a $ae^n(n+1) \geqslant 1$, donc $ae^n(n+1) \leqslant (ae^n(n+1))^p$ et enfin

$$|J| \leqslant (ae^n(n+1)n^n)^p.$$

D'autre part, puisque $(p-1)!$ divise J et que $J \neq 0$ pour p premier assez grand, on a $(p-1)! \leqslant |J|$. Or pour tout $C > 0$, on a $\lim_{p\to\infty} \frac{C^p}{(p-1)!} = 0$. Pour p premier assez grand, on a alors $C^p < (p-1)!$. En prenant $C = ae^n(n+1)n^n$, on a une contradiction.

Donc il n'existe pas d'entiers $a_0,\ldots,a_n$ tels que $a_0 + a_1 e + \cdots + a_n e^n = 0$ avec $a_0 \neq 0$. Si e était algébrique, il serait racine d'un polynôme P_0 à coefficients rationnels, et en le multipliant par les produit des numérateurs des coefficients de P_0, e serait aussi racine d'un polynôme de $\mathbb{Z}[X]$. Quitte à diviser P_0 par X^r, on peut supposer que $a_0 \neq 0$. Le réel e est donc transcendant.