NOMBRES ALGÉBRIQUES – NOMBRES TRANSCENDANTS

1. En guise d'introduction

Il a fallu bien longtemps pour comprendre la nature profonde de l'ensemble de nombres qui nous est le plus familier après $\mathbb{N}$, à savoir le corps $\mathbb{R}$ des nombres réels. Pendant des siècles, la perception intuitive de ce que sont une droite et les points qui la constituent s'est avérée amplement suffisante. Vingt siècles avant nous, les Grecs avaient déjà compris que tout nombre n'est pas rationnel en prouvant par des arguments géométriques l'irrationalité de la diagonale du carré unité. Dès lors, on a admis comme une évidence l'existence et les propriétés de cet ensemble $\mathbb{R}$ qui se représentait si bien par les points d'une droite.

Pourtant, dès le début du XIX$^{\text{ème}}$ siècle, la nécessité d'un véritable formalisme mathématique (notamment en analyse) a conduit les plus illustres mathématiciens à remettre en cause quelques « évidences », et en tout premier lieu la principale d'entre elles : ce qu'est véritablement un nombre réel. Car sans une compréhension profonde de ce qu'est $\mathbb{R}$, comment prouver quelque théorème d'analyse que ce soit avec un tant soit peu de rigueur ? L'exemple le plus simple et le plus caricatural est bien celui du théorème des valeurs intermédiaires, dont une multitude de preuves ont été proposées (dès lors que le concept de "fonction continue", grâce notamment à Bolzano, a été à peu près bien compris), preuves toutes incomplètes puisque ce théorème résulte de la nature topologique profonde de $\mathbb{R}$. À titre d'exemple, on pourra citer la preuve due à Cauchy de ce théorème ; à peu de choses près, Cauchy écrit : *si une fonction $f(x)$ reste continue entre des limites $x = x_0$ et $x = X$, il est évident que si, en faisant croître la variable x par degrés insensibles depuis la première limite jusqu'à la seconde, la fonction $f(x)$ passe de valeurs négatives à des valeurs positives, alors il ne se peut qu'elle ne s'évanouisse pour une certaine valeur de la variable x.* Fin de la démonstration ! (au passage, c'est joli de dire « s'évanouir » au lieu de « s'annuler », non ?).

Ce n'est que vers la fin du XIX$^{\text{ème}}$ siècle que deux immenses mathématiciens, Cantor et Dedekind, donneront à peu près simultanément une présentation rigoureuse de ce qu'est $\mathbb{R}$. Chacun aura sa propre approche du problème, mais les ensembles ainsi construits sont les mêmes, et correspondent à ce que notre intuition demande. Cantor, constatant que certaines suites « de Cauchy » de rationnels ne convergent pas dans $\mathbb{Q}$, va prendre sa truelle et son sac de ciment et, en quelque sorte, « boucher les trous » de $\mathbb{Q}$ (une construction de $\mathbb{R}$ suivant les idées de Cantor est disponible en suivant le lien suivant : https://www.dropbox.com/s/z8n0r72kcjoeqis/R.pdf). Dedekind quant à lui, notant que certaines parties non vides majorées de $\mathbb{Q}$ ne possèdent pas de borne supérieure (comme par exemple $A = \left\{x \in \mathbb{Q} \ / \ x^2 < 2\right\}$), va se déguiser en charpentier et « clore » ces parties en appelant « nombre réel » un machin qui vient les fermer supérieurement (le réel $\sqrt{2}$ dans notre exemple).

Cependant, une autre approche naïve de ce qu'est $\mathbb{R}$, que certains ont tentée, pourrait être la suivante : comme les Grecs l'ont vu, il manque des choses à $\mathbb{Q}$ telles que $\sqrt{2}$ et autres nombres du même style. Pourquoi alors ne pas rajouter à $\mathbb{Q}$ tous les nombres envisageables comme $\sqrt[3]{7}$, $\sqrt[17]{921}$, ainsi que tous ceux obtenus à partir de ceux-là par sommes, produits, quotients, plus quelques radicaux de-ci de-là pour faire joli, du genre $\sqrt{\sqrt[4]{68} + \sqrt[3]{3 - \sqrt{5}}}$ … *a priori*, tout cela commence à faire du monde et ce serait bien le diable si $\mathbb{R}$, au bout du compte, n'était pas l'ensemble de ces gens-là ! Mais à y regarder de plus près, ces nombres ainsi construits ont une particularité : on peut, en bidouillant pas mal et pas toujours de manière aisée (cf. exemple à suivre), fabriquer un polynôme dont ils sont racine et dont les coefficients sont rationnels. Et les mathématiciens se sont assez vite convaincus qu'il y avait probablement des nombres autres, qui n'avaient pas cette particularité d'être racines de polynômes rationnels. Cette vision naïve de $\mathbb{R}$ était donc vraisemblablement insuffisante. Finalement, c'est Liou-

ville qui donnera le coup de grâce à cette approche en construisant pour la première fois en 1844 un exemple explicite de nombre *transcendant*, c'est à dire qui n'est racine d'aucune équation algébrique rationnelle.

Exemple : soit $x = \sqrt{7} - 2\sqrt[3]{4}$.

Alors : $(x - \sqrt{7})^3 = (-2\sqrt[3]{4})^3 = -32$, soit encore $x^3 - 3\sqrt{7}x^2 + 3\sqrt{7}^2 x - \sqrt{7}^3 = -32$. Je réécris cette équation ainsi : $x^3 + 21x + 32 = \sqrt{7}(3x^2 + 7)$ et il n'y a plus qu'à élever au carré pour découvrir, oh joie !, que x vérifie l'équation algébrique à coefficients rationnels :

$$(x^3 + 21x + 32)^2 = 7(3x^2 + 7)^2$$

ce qui, aux erreurs de calcul près, donne :

$$x^6 - 21x^4 + 64x^3 + 147x^2 + 1344x + 681 = 0 \quad !!!$$

2. Nombres algébriques

Par définition, un réel a est *algébrique* s'il existe un polynôme P, non nul, à coefficients rationnels, tel que $P(a) = 0$. En multipliant un tel polynôme par le plus petit commun multiple des dénominateurs de ses coefficients, on peut voir que les nombres algébriques sont aussi les racines des polynômes non nuls à coefficients *entiers*.

Si l'on regarde de près l'exemple précédent, notre x est la somme de deux nombres algébriques, $\sqrt{7}$ et $-2\sqrt[3]{4}$, qui sont tous deux racines des polynômes très simples que sont $X^2 - 7$ et $X^3 + 32$. Pourtant, le polynôme que l'on a trouvé et dont x est racine n'est pas précisément simple, et ne possède aucun lien direct avec les polynômes $X^2 - 7$ et $X^3 + 32$! Et le pire est que ça ne s'est pas trop mal passé parce que si l'on était partis de $y = \sqrt[3]{7} - 2\sqrt[5]{4}$, il aurait probablement fallu aller dénicher un polynôme de degré 15 !

On peut cependant prouver grâce à l'algèbre linéaire (et non par le calcul, comme je viens de le suggérer), le théorème suivant :

> Théorème : l'ensemble des nombres algébriques est un corps.

Ainsi, une somme, un produit, un quotient de nombres algébriques donnent un nombre algébrique.

Afin de ne pas alourdir ce polycopié dont la vocation initiale est plutôt culturelle, la preuve de ce théorème est renvoyée à la fin.

3. Tout réel n'est pas algébrique

Par définition, nous dirons d'un réel x qu'il est *transcendant* s'il n'est pas algébrique. Comme on l'a dit, Liouville donnera au début du XIX$^{\text{ème}}$ siècle le premier exemple explicite de nombre transcendant. Cet exemple sera détaillé au paragraphe suivant. En attendant, nous allons donner ici une preuve due à Cantor, historiquement plus tardive, du fait qu'il existe des nombres transcendants. Cette preuve a ceci d'intéressant qu'elle va plus loin qu'un simple résultat d'existence : elle dit en outre que *presque tous* les nombres réels sont transcendants, mais elle a ceci de très étrange que, contrairement à celle de Liouville, elle n'en exhibe pas un seul !

Rappelons qu'un ensemble *dénombrable* est un ensemble qui est en bijection avec $\mathbb{N}$ ou avec une partie de $\mathbb{N}$; en quelque sorte, cela correspond au concept intuitif d'ensemble dont on peu « numéroter » les éléments. On sait, c'est par exemple une application de l'écriture décimale des nombres réels, que $\mathbb{R}$ n'est pas un ensemble dénombrable et donc que son infini est « beaucoup plus grand » que celui de $\mathbb{N}$. Nous allons prouver ici que l'ensem-

ble A des réels algébriques est dénombrable. Il en résultera bien évidemment qu'il existe des réels non algébriques, donc transcendants, et même que ceux-ci sont très largement majoritaires !

Soit $P = a_p X^p + \ldots + a_0$ un polynôme à coefficients entiers de degré p.

Posons $\nu(P) = p + \sum_{k=0}^{p} |a_k|$ (l'entier $\nu(P)$ s'appelle le poids du polynôme P).

Remarquons que pour tout entier naturel n, il n'existe qu'un nombre fini de polynômes de poids égal à n (car un polynôme de poids n a son degré majoré par n, et chacun de ses coefficients est un entier majoré par n en valeur absolue, ce qui ne lui laisse qu'un nombre fini de valeurs possibles), et que chacun de ces polynômes n'a qu'un nombre fini de racines réelles. Pour numéroter les réels algébriques, il suffit (!) donc de mettre en place le processus suivant : on liste les racines réelles de tous les polynômes de poids 1, il n'y en a qu'un nombre fini, et on les numérote dans l'ordre croissant ; puis on passe aux racines des polynômes de poids 2, que l'on numérote à la suite en ne renumérotant pas celles que l'on avait éventuellement déjà rencontrées. On passe ensuite aux racines des polynômes de poids 3 et ainsi de suite. Au total, on aura donné ainsi un numéro à tous les réels algébriques : l'ensemble qu'ils constituent est dénombrable.

4. Le théorème de Liouville

Soit a un nombre algébrique irrationnel, et P un polynôme non nul à coefficients rationnels *de degré minimum* dont a est racine. Le degré d de ce polynôme P est appelé *degré du nombre algébrique a.*

Notons que P ne saurait posséder de racine rationnelle r, sans quoi après factorisation par $X - r$ et compte-tenu du fait que a est supposé irrationnel, donc que $a \neq r$, on trouverait un polynôme rationnel de degré plus petit dont a est racine.

Comme on l'a déjà dit, quitte à multiplier par le ppcm des dénominateurs de ses coefficients, on pourra supposer que P est à coefficients entiers.

Soit alors un rationnel $\frac{p}{q}$. Il est évident que $q^d P(\frac{p}{q}) = q^d (a_d \frac{p^d}{q^d} + \ldots + a_1 \frac{p}{q} + a_0)$ est entier puisque les a_i le sont, et comme P ne possède pas de racine rationnelle, cet entier est non nul.

Or il existe un théorème délicat et méconnu qui dit qu'un entier non nul est, en valeur absolue, plus grand que 1 ! Il vient donc $\left|q^d P(\frac{p}{q})\right| \geq 1$, soit $\left|P(\frac{p}{q})\right| \geq \frac{1}{q^d}$.

Mais il ne faut pas oublier que a est racine de P. Alors grâce à l'inégalité des accroissements finis, si l'on note m un majorant de $|P'|$ sur $[a-1, a+1]$, il vient :

$$\frac{1}{q^d} \leq \left|P(\frac{p}{q})\right| = \left|P(a) - P(\frac{p}{q})\right| \leq m\left|a - \frac{p}{q}\right| \quad \text{et ce dès que } \left|a - \frac{p}{q}\right| \leq 1 .$$

On a finalement prouvé le théorème de Liouville, qui dit en quelque sorte qu'il existe une limitation dans la qualité des approximations d'un nombre algébrique par des rationnels :

Théorème (Liouville) : soit a un réel algébrique irrationnel de degré d. Alors il existe une constante strictement positive k telle que, pour tout rationnel $\frac{p}{q}$ vérifiant $\left|a - \frac{p}{q}\right| \leq 1$, on ait $\left|a - \frac{p}{q}\right| \geq \frac{k}{q^d}$.

L'idée de Liouville est alors de construire un nombre réel qui s'approche extrêmement bien par des rationnels de dénominateur relativement petit, trop bien pour respecter la limitation imposée par son théorème aux nombres algébriques.

Soit L le nombre suivant :

$$L = \sum_{n=1}^{+\infty} \frac{1}{10^{n!}} .$$

L est le nombre dont l'écriture décimale ne comporte presque que des 0 avec quelques rares 1, disposés aux rangs 1, 2, 6, 24, 120, 720, … $n!$,… derrière la virgule. Notons que cette écriture décimale ne devenant pas périodique, L est irrationnel.

Posons $L_p = \sum_{n=1}^{p} \frac{1}{10^{n!}}$. Il est clair que L_p est une excellentissime approximation rationnelle de L : songez par exemple que L et L_6 ont leurs 5039 premières décimales en commun !

Évidemment, on a $\left|L - L_p\right| \leq 1$ et L_p peut s'écrire $\frac{\text{entier}}{10^{p!}}$.

Supposons alors que L est algébrique de degré d .

D'après le théorème de Liouville, on devrait avoir l'existence d'une constante strictement positive k telle que

$$\left|L - L_p\right| \geq \frac{k}{q^d} = \frac{k}{(10^{p!})^d} .$$

Mais il est clair que $\left|L - L_p\right| \leq \frac{2}{10^{(p+1)!}}$.

On a donc $\frac{k}{(10^{p!})^d} \leq \frac{2}{10^{(p+1)!}}$, soit $k \leq \frac{2}{10^{p!(p+1-d)}}$ et ce pour tout entier p. Il n'y a plus qu'à faire tendre p vers l'infini pour récupérer $k \leq 0$ ce qui est contraire à nos hypothèses. L est donc un nombre transcendant.

Théorème (Liouville) : Le nombre $L = \sum_{n=1}^{+\infty} \frac{1}{10^{n!}}$ est transcendant.

5. Des exemples de nombres transcendants

Le plus simple, le plus étrange, mais aussi le plus facile à mémoriser, est sans doute le nombre de Champernowne $c = 0{,}1234567891011121314...$ (obtenu en écrivant à la suite les entiers successifs par leur écriture décimale).

Hermite a, le premier, montré la transcendance d'un nombre non artificiellement construit pour cela, en prouvant en 1873 que e, la base des logarithmes népériens, est transcendant.

En s'inspirant très fortement des travaux d'Hermite, Lindemann montre neuf ans plus tard la transcendance de π , prouvant du même coup l'impossibilité de la quadrature du cercle.

On connaît à l'heure actuelle des familles assez vastes de nombres transcendants, mais tout cela ne s'obtient pas sans peine car il s'agit d'une théorie mathématique difficile.

Théorème (Baker) : si a est un réel algébrique strictement positif différent de 1, $\ln a$ est transcendant.

Ainsi $\ln 2$, $\ln 3$ … sont des nombres transcendants.

Théorème (Gelfond-Schneider) : si a est un réel algébrique strictement positif différent de 1, et si b est un nombre algébrique irrationnel, alors a^b est transcendant.

Ainsi, $2^{\sqrt{2}}$ est transcendant.

Le théorème de Gelfond-Schneider est délicat ; sa preuve utilise (entre autres !) le principe des tiroirs (ou des trous de pigeons) de Dirichlet selon lequel, si l'on dispose de n tiroirs et de $n+1$ chaussettes, alors l'un des tiroirs contient au moins deux chaussettes.

6. La quadrature du cercle

Comme on l'a dit plus haut, Lindemann, en prouvant la transcendance de π, a du même coup prouvé l'impossibilité de la quadrature du cercle. Ce problème, qui nous a été légué par les Grecs il y a un peu plus de 2000 ans, consiste à construire un carré de même aire qu'un disque donné en n'utilisant qu'une règle (non graduée) et un compas.

Ce paragraphe a pour objectif de faire le lien entre ces deux résultats en apparence totalement étrangers, l'un de théorie des nombres, l'autre de géométrie.

Le plan affine euclidien est rapporté à un repère orthonormé $(0,\vec{i},\vec{j})$ dans lequel on écrit tous les systèmes de coordonnées et toutes les équations de droites et de cercles envisagés. Alors :

Théorème : Les coordonnées d'un point constructible à la règle et au compas sont des réels algébriques.

Supposons momentanément ce théorème prouvé. Donnons-nous alors un cercle dans le plan euclidien, que l'on peut toujours supposer être le cercle unité (quitte à changer d'unité de longueur). La base du carré à construire ayant une longueur égale à $\sqrt{\pi}$, il s'agit de construire à la règle et au compas deux points distants de $\sqrt{\pi}$, ce qui permet alors grâce au compas de construire le point de coordonnées $(\sqrt{\pi},0)$. D'après notre théorème, le réel $\sqrt{\pi}$ est donc algébrique, et comme le produit de deux algébriques en est un (cf. le paragraphe 2), $\pi=\sqrt{\pi}\sqrt{\pi}$ aussi est algébrique, ce que dément Lindemann. L'impossibilité de la quadrature du cercle est ainsi prouvée.

Reste à expliquer ce théorème quelque peu mystérieux, et en réalité ce n'est pas si difficile ; nous allons pour ce faire raisonner par récurrence.

Au départ, on ne dispose que des points 0 et I, de coordonnées respectives $(0,0)$ et $(1,0)$. Ces deux points seront dits « construits à l'étape 0 ».

On définit alors par récurrence les points « construits à l'étape n » comme étant tous les points que l'on obtient comme intersections droite-droite ou droite-cercle ou cercle-cercle de droites passant par deux points construits à l'étape $n-1$, et de cercles centrés en des points construits à l'étape $n-1$ et de rayon la distance entre deux points construits à l'étape $n-1$.

À titre d'exemple, comme on ne peut tracer à partir des points 0 et I que la droite passant par ces deux points ainsi que deux cercles (celui centré en 0 passant par I et celui centré en I passant par 0), les points construits à l'étape 1 sont au nombre de 6 : les points 0, I, ainsi que ceux de coordonnées $(-1,0)$, $(2,0)$, $\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)$ et $\left(\frac{1}{2},-\frac{\sqrt{3}}{2}\right)$.

Bien entendu, un point du plan sera dit « constructible à la règle et au compas » s'il est constructible en n étapes pour une certaine valeur de l'entier n.

Il s'agit maintenant de prouver par récurrence que l'on ne construit ainsi que des points dont les coordonnées sont des réels algébriques.

Les deux points de départ 0 et I sont bien à coordonnées algébriques, ainsi d'ailleurs que les points construits à l'étape 1.

Supposons que pour un certain entier n, tous les points construits à l'étape n soient à coordonnées algébriques.

Écrivons alors l'équation d'une droite passant par deux points construits à l'étape n, et d'un cercle centré en un point construit à l'étape n et de rayon la distance entre deux points construits à l'étape n :

$$(D) \ : \ y - y_A = \frac{y_B - y_A}{x_B - x_A}(x - x_A) \qquad ; \qquad (C) \ : \ (x - x_C)^2 + (y - y_C)^2 = (x_D - x_E)^2 + (y_D - y_E)^2 .$$

Tous les coefficients $x_A, y_A, \ldots, x_E, y_E$ sont supposés être algébriques par hypothèse de récurrence.

Imaginons maintenant que l'on cherche l'intersection de deux droites ou de deux cercles ou d'une droite et d'un cercle du type précédent. On va alors être amené à résoudre des équations du premier degré (intersection droite-droite) ou du second degré (intersection droite-cercle ou cercle-cercle) dont les coefficients sont tous algébriques. Les formules de résolution ne feront donc apparaître que des nombres algébriques, voire à la rigueur des racines carrées (quand on résout une équation du second degré) de nombres algébriques. Or il est évident que la racine carrée d'un nombre algébrique est elle-aussi un nombre algébrique (si a est racine de P à coefficients rationnels, $\sqrt{a}$ est racine de $P(X^2)$ qui est lui-aussi à coefficients rationnels). Finalement, les coordonnées du point d'intersection cherché seront à leur tour des nombres algébriques puisque ceux-ci, comme on l'a vu, constituent un corps. On a ainsi prouvé que tout point construit à l'étape $n+1$ est à coordonnées algébriques, ce qui achève notre récurrence.

Remarque : on peut prouver, en raffinant un peu la démonstration précédente, un résultat plus précis. Non seulement un nombre constructible doit être algébrique, mais en plus le degré minimum d'un polynôme rationnel non nul dont il est racine doit être une puissance de 2 (ce n'est qu'une condition nécessaire). Il en résulte que les nombres $\sqrt[3]{2}$, $\cos\frac{2\pi}{7}$ *et* $\cos\frac{2\pi}{9}$ *(dont on peut prouver qu'ils sont chacun solutions d'une équation irréductible de degré 3 à coefficients rationnels) ne sont pas constructibles à la règle et au compas : une conséquence de cela est que le problème général de la trisection de l'angle n'a pas de solution, puisque l'on peut facilement construire à la règle et au compas le polygone régulier à 3 côtés, mais pas celui à 9 côtés. Pour préciser tout cela, un problème est disponible ici :*
https://dl.dropbox.com/u/40341647/construction%20%C3%A0%20la%20r%C3%A8gle%20et%20au%20compas.pdf

7. Un exercice : la transcendance de e

On suppose que e est un réel algébrique, et l'on désigne par $a_0, a_1, \ldots, a_n$ des entiers avec $a_n \neq 0$ tels que :

$$a_0 + a_1 \mathrm{e} + \ldots + a_n \mathrm{e}^n = 0 .$$

a. Pour tout polynôme Q de $\mathbb{R}[X]$, on note $D(Q) = \sum_{k=0}^{+\infty} Q^{(k)}$ et pour tout réel t, $I(t) = \int_0^t \mathrm{e}^{t-u} Q(u) \mathrm{d}u$.

Prouver que :

$$I(t) = \int_0^t \mathrm{e}^{t-u} Q(u) \mathrm{d}u = \mathrm{e}^t D(Q)(0) - D(Q)(t) .$$

b. On choisit désormais $Q = X^{p-1}(X-1)^p \ldots (X-n)^p$ où p est un nombre premier, et l'on pose :

$$J = a_0 I(0) + a_1 I(1) + \ldots + a_n I(n)\,.$$

Prouver que J est un entier, qu'il est divisible par $(p-1)!$, et qu'il n'est pas divisible par $p!$ pour p premier assez grand.

c. Prouver l'existence d'une constante k telle que l'on ait $|J| \leq k^p$, et conclure.

8. Les nombres algébriques constituent un corps

Pour prouver le résultat annoncé, nous allons au préalable donner une caractérisation utile des nombres algébriques.

Soit un réel α, et $\mathbb{Q}[\alpha] = \{P(\alpha),\, P \in \mathbb{Q}[X]\}$. Il est à peu près évident que $\mathbb{Q}[\alpha]$ est un $\mathbb{Q}$-espace vectoriel, dont une famille génératrice est $(\alpha^n)_{n\in\mathbb{N}}$. Si $\mathbb{Q}[\alpha]$ est de dimension finie sur $\mathbb{Q}$, alors en notant p cette dimension, la famille de $p+1$ éléments qu'est $(1,\alpha,\ldots,\alpha^p)$ est liée et il existe donc des scalaires non tous nuls $a_0, a_1, \ldots, a_p$ tels que l'on ait $a_0 + a_1\alpha + \ldots + a_p\alpha^p = 0$: cette égalité traduit exactement que α est racine d'un polynôme rationnel non nul, c'est à dire que α est algébrique.

Réciproquement, supposons α algébrique, et soit π un polynôme rationnel de degré p dont α est racine. Pour tout polynôme P de $\mathbb{Q}[X]$, effectuons la division euclidienne de P par π : $P = Q\pi + R$ avec $\deg R < \deg \pi$. En évaluant en α et compte-tenu du fait que α est racine de π, il vient $P(\alpha) = R(\alpha)$: tout polynôme rationnel en α s'exprime donc comme un polynôme en α de degré plus petit que $p-1$. Il vient donc $\mathbb{Q}[\alpha] = \{R(\alpha),\, \deg R < p\} = \text{vect}(1,\alpha,\ldots,\alpha^{p-1})$, de sorte que $\mathbb{Q}[\alpha]$ est de dimension finie sur $\mathbb{Q}$.

On a ainsi prouvé l'important résultat suivant :

> Propriété 1 : un réel α est algébrique si et seulement si $\mathbb{Q}[\alpha]$ est un $\mathbb{Q}$-espace vectoriel de dimension finie.

Fixons alors un réel algébrique α. Il est facile de voir que la somme et le produit de deux polynômes rationnels en α est un polynôme rationnel en α, de sorte que $\mathbb{Q}[\alpha]$ est un anneau. Considérons un élément non nul x_0 de $\mathbb{Q}[\alpha]$ et envisageons l'application :

$$\begin{array}{ccc} \mathbb{Q}[\alpha] & \to & \mathbb{Q}[\alpha] \\ x & \mapsto & x_0 x \end{array}.$$

Cette application est manifestement linéaire, injective puisque x_0 est non nul, et comme $\mathbb{Q}[\alpha]$ est de dimension finie elle est surjective. 1 possède donc un antécédent, ce qui signifie que $1/x_0$ est dans $\mathbb{Q}[\alpha]$: $\mathbb{Q}[\alpha]$ est un corps.

> Propriété 2 : si α est algébrique, alors $\mathbb{Q}[\alpha]$ est un corps.

Reste à franchir la dernière étape, peut-être la plus délicate, pour prouver que les réels algébriques constituent un corps. Pour cela, il s'agit de prouver que la somme (ou le produit) de deux algébriques en est un, car le fait que l'inverse d'un nombre algébrique non nul est un nombre algébrique est tout à fait évident (il suffit de mettre en facteur α à une puissance convenable dans un polynôme dont α est racine).

Fixons donc deux réels algébriques α et β, et envisageons $\mathbb{Q}[\alpha,\beta] = \{P(\alpha,\beta),\, P \in \mathbb{Q}[X,Y]\}$. Un polynôme rationnel en α et β pouvant facilement être vu comme un polynôme en β à coefficients dans $\mathbb{Q}[\alpha]$, on a $\mathbb{Q}[\alpha,\beta] = \mathbb{Q}[\alpha][\beta]$. Mais α étant algébrique sur $\mathbb{Q}$, il est racine d'un polynôme non nul à coefficients dans $\mathbb{Q}$,

donc dans $\mathbb{Q}[\alpha]$ qui est un corps. En reprenant les arguments de la preuve de la propriété 1, il vient donc que $\mathbb{Q}[\alpha,\beta]=\mathbb{Q}[\alpha][\beta]$ est de dimension finie si on le voit comme un $\mathbb{Q}[\alpha]$-espace vectoriel. $\mathbb{Q}[\alpha]$ étant lui-même de dimension finie sur $\mathbb{Q}$, il vient (c'est le théorème classique dit « de la base télescopique ») que $\mathbb{Q}[\alpha,\beta]=\mathbb{Q}[\alpha][\beta]$ est de dimension finie sur $\mathbb{Q}$. Nous noterons p cette dimension.

Posons alors $s=\alpha+\beta$. Comme s est dans $\mathbb{Q}[\alpha,\beta]$, la famille $(1,s,\dots,s^p)$ est liée ce qui donne, comme on l'a déjà vu, l'existence d'un polynôme rationnel non nul dont s est racine : s est algébrique. On raisonne de même pour le produit $\alpha\beta$.