Université P. et M. Curie (Paris VI) date de mise à jour: 19/03/2009
Deuxième semestre 2008/2009

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales

Deuxième fascicule : 26/01/2009

1 Approximation diophantienne, irrationalité et transcendance

1.1 Nombres : rationnels, irrationnels

Les *nombres* que nous allons étudier sont les nombres complexes. Leur construction se fait en plusieurs étapes : partant des entiers naturels $\mathbf{N} = \{0, 1, 2, 3, \cdots\}$, on construit l'*anneau des entiers rationnels* $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$ de façon à ce que chaque élément ait un inverse pour l'addition, puis le *corps des nombres rationnels* $\mathbf{Q} = \{a/b\ ;\ a \in \mathbf{Z},\ b \in \mathbf{Z}_{>0}\}$ de telle sorte que chaque élément non nul ait un inverse pour la multiplication. Chaque nombre rationnel a une unique représentation p/q avec $p \in \mathbf{Z}$ et $q \in \mathbf{Z}_{>0}$ sans facteur commun : $\mathrm{pgcd}(p, q) = 1$.

L'étape suivante est la construction des *nombres réels* : alors que les constructions précédentes étaient de nature algébrique, celle de $\mathbf{R}$ fait intervenir la notion topologique de limite : $\mathbf{R}$ *est le complété de* $\mathbf{Q}$ pour la topologie usuelle sur les rationnels. La dernière étape, la construction de $\mathbf{C}$ à partir de $\mathbf{R}$, est de nouveau de nature algébrique : $\mathbf{C}$ *est la clôture algébrique de* $\mathbf{Q}$, tout polynôme non constant admet au moins une racine complexe.

Un *nombre irrationnel* est un nombre qui n'est pas dans $\mathbf{Q}$. L'ensemble de ces nombres ne jouit pas de bonnes propriétés algébriques : la somme de nombres irrationnels peut être rationnelle ou irrationnelle, le produit de deux nombres irrationnels peut être rationnel ou irrationnel. En revanche la somme d'un nombre rationnel et d'un nombre irrationnel est un nombre irrationnel ; le produit d'un nombre rationnel *non nul* et d'un nombre irrationnel est un nombre irrationnel. La racine carrée (et plus généralement la racine k-ième, pour $k \geq 1$) d'un nombre irrationnel est un nombre irrationnel. Mais le carré d'un nombre irrationnel peut être rationnel ou irrationnel.

Le fait que $\mathbf{R}$ contienne strictement $\mathbf{Q}$ est bien connu : il existe des nombres irrationnels. Un des exemples les plus anciens est celui de $\sqrt{2}$. La démonstration la plus connue se fait par l'absurde : si p/q est un nombre rationnel dont le carré est 2 avec $\mathrm{pgcd}(p, q) = 1$, la relation $p^2 = 2q^2$ implique que p est pair, disons $p = 2a$, puis en simplifiant par 2 la relation $2a^2 = q^2$ montre que q est pair, ce qui est une contradiction.

Une démonstration géométrique se fait de la façon suivante : considérons un rectangle dont les côtés sont $1 + \sqrt{2}$ et 1. Comme le grand côté $1 + \sqrt{2}$ est dans l'intervalle $(2, 3)$, on peut décomposer ce premier rectangle en deux carrés de côté 1 plus un petit rectangle dont le grand côté est 1, et le petit côté $\sqrt{2} - 1$. On remarque alors que les proportions de ce second rectangle sont les mêmes que celles du rectangle initial :

$$\frac{1}{\sqrt{2} - 1} = 1 + \sqrt{2}.$$

par conséquent si on répète cette construction à partir du second carré, on obtiendra de nouveau deux carrés de côtés $\sqrt{2}-1$ et un troisième rectangle dont la proportion des longueurs des côtés sera toujours la même. Par conséquent le processus ne s'arrête pas.

En revanche si on part d'un rectangle dont les côtés sont entiers, la construction précédente va produire des rectangles de plus en plus petits dont les côtés sont toujours des entiers, donc le processus s'arrêtera au bout d'un temps fini (il ne reste plus de petit rectangle). Il en est de même pour tout rectangle dont les proportions sont rationnelles : si le rapport du grand côté par le petit côté est a/b avec $b>0$, on prend comme unité de mesure celle qui donne au petit côté la longueur b, et alors les deux côtés ont des longueurs entières.

Cette démonstration fait intervenir le *développement en fraction continue* d'un nombre réel x. On écrit

$$x=[x]+\{x\} \quad \text{avec } [x]\in\mathbf{Z} \text{ et } 0\le\{x\}<1.$$

Si x n'est pas entier, alors $\{x\}>0$ et le nombre $x_1=1/\{x\}$ est >1. Posons $a_0=[x]$, $a_1=[x_1]$. Par exemple quand x est >0 le nombre a_0 est le nombre maximal de carrés de côtés 1 que l'on peut disposer côte–à–côte dans un rectangle de côtés 1 et x, tandis que a_1 est le nombre maximal de carrés de côtés $\{x\}$ dans le second rectangle qui reste. Par récurrence on définit une suite $(x_n)_{n\ge1}$ de nombres réels >1 et une suite $(a_n)_{n\ge1}$ de nombres entiers ≥1 (éventuellement finies) de la façon suivante : si x_{n-1} n'est pas entier, on pose $x_n=1/\{x_{n-1}\}$ et $a_n=[x_n]$, ce qui donne

$$x=a_0+\frac{1}{x_1},\quad x_1=a_1+\frac{1}{x_2},\quad \cdots,\quad x_n=a_n+\frac{1}{x_{n+1}}\cdots$$

On peut donc écrire

$$x=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\{x_2\}}}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots\,a_{n-1}+\cfrac{1}{a_n+\{x_n\}}}}}$$

avec $0\le\{x_n\}<1$. La construction s'arrête au premier pas si x est entier : on obtient seulement $x=a_0$. Si x n'est pas entier mais si x_n est entier pour un entier $n\ge1$ alors $a_n=x_n$ et $\{x_n\}=0$. Noter que la condition $x_n>1$ entraîne $a_n\ge2$. Il est clair que si la construction s'arrête, alors x est rationnel. Inversement, si x est rationnel l'argument géométrique avec les rectangles montre que la construction s'arrêtera au bout d'un nombre fini d'étapes. Un nombre rationnel admet deux représentations sous forme d'une telle fraction, l'une dont le dernier terme a_n est ≥2, l'autre avec un terme de plus et $a_{n+1}=1$: en effet on peut écrire un entier $a\ge2$ sous la forme $(a-1)+(1/1)$.

On montre [6] que tout nombre réel irrationnel x admet une unique représentation sous forme d'une fraction continue infinie

$$x=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots\,a_{n-1}+\cfrac{1}{a_n+\cfrac{1}{\ddots}}}}} \tag{1.1}$$

avec des coefficients a_n entiers rationnels satisfaisant $a_n \geq 1$ pour $n \geq 1$, et inversement pour toute suite $(a_n)_{n\geq 0}$ d'entiers rationnels avec $a_n \geq 1$ pour $n \geq 1$, la fraction continue (1.1) définit un nombre réel irrationnel.

Pour simplifier l'écriture on écrit cette fraction continue sous l'une des formes suivante :

$$x = [a_0; a_1, a_1, a_2, \ldots, a_n, \ldots] \quad \text{ou} \quad x = a_0 + \frac{1}{|a_1+} \; \frac{1}{|a_2+} \; \cdots \; \frac{1}{|a_n+} \; \cdots$$

Un exemple, dû à Euler, est le développement en fraction continue du nombre e :

$$e = [2;\, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots] = 2 + \frac{1}{|1+} \; \frac{1}{|2+} \; \frac{1}{|1+} \; \frac{1}{|1+} \; \frac{1}{|4+} \; \frac{1}{|1+} \; \frac{1}{|1+} \; \frac{1}{|6+} \; \frac{1}{|1+} \; \cdots$$

Voici une démonstration de l'irrationalité du nombre e est due à Fourier (cours à l'école Polytechnique, 1815).

Proposition 1.2. *Le nombre*

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} + \cdots$$

est irrationnel.

Démonstration. Soit N un entier positif. On tronque la série définissant e. Soit N un entier positif. On a

$$N!\, e - \sum_{n=0}^{N} \frac{N!}{n!} = \sum_{k\geq 1} \frac{N!}{(N+k)!}. \tag{1.3}$$

Le membre de droite de (1.3) est une somme de nombres positifs, donc n'est pas nul. De la minoration du coefficient binomial

$$\frac{(N+k)!}{N!k!} \geq N+1 \quad \text{pour } k \geq 1,$$

on déduit

$$\sum_{k\geq 1} \frac{N!}{(N+k)!} \leq \frac{1}{N+1} \sum_{k\geq 1} \frac{1}{k!} = \frac{e-1}{N+1}.$$

Par conséquent le membre de droite de (1.3) tend vers 0 quand N tend vers l'infini. Dans le membre de gauche, $N!$ et $\sum_{n=0}^{N} N!/n!$ sont des entiers. Il en résulte que $N!e$ n'est jamais un entier, donc e est un nombre irrationnel.

□

Exercice. a) En adaptant cet argument, montrer que le nombre e n'est pas racine d'un polynôme de degré 2 à coefficients rationnels.
`Indication` : un nombre quadratique x est racine d'une équation $ax + b + cx^{-1} = 0$ avec a, b, c entiers rationnels non tous nuls.
Référence : J. Liouville – *Sur l'irrationalité du nombre* $e = 2,718\ldots$, J. Math. Pures Appl. (1) **5** (1840), p. 192.
`http ://portail.mathdoc.fr/JMPA/`

b) Montrer que le nombre $e^{\sqrt{2}}$ est irrationnel.
`Indication` : Montrer plus précisément que $e^{\sqrt{2}} + e^{\sqrt{-2}}$ est irrationnel. On pourra vérifier que les nombres $(2N)!/2^{N-m}(2m)!$ $(0 \le m \le N)$ sont entiers.
c) Montrer que e^2 n'est pas racine d'un polynôme de degré 2 à coefficients rationnels.
`Indication` : On pourra montrer que les nombres

$$\frac{N!}{2^{N-n-1}n!}, \quad (0 \le n \le N)$$

sont entiers pour une infinité de N.
Référence : J. Liouville – *Addition à la note sur l'irrationalité du nombre e*, J. Math. Pures Appl. (1) **5** (1840), p. 193–194.
`http ://portail.mathdoc.fr/JMPA/`
d) Montrer que le nombre $e^{\sqrt{3}}$ est irrationnel.
e) Soit $(a_n)_{n\ge 0}$ une suite bornée de nombres entiers. Montrer que les conditions suivantes sont équivalentes :
(i) Il existe $N_0 > 0$ tel que $a_n = 0$ pour tout $n \ge N_0$.
(ii) Le nombre

$$\vartheta_1 = \sum_{n\ge 0} \frac{a_n}{n!}$$

est rationnel
(iii) Le nombre

$$\vartheta_2 = \sum_{n\ge 0} \frac{a_n 2^n}{n!}$$

est rationnel.

1.2 Critère d'irrationalité

La démonstration d'irrationalité de Fourier que nous venons de donner utilise le fait qu'un nombre rationnel ne possède pas de bonne approximation rationnelle autre que lui-même. En effet, si ϑ est rationnel, on l'écrit a/b avec $b > 0$ et alors, pour tout $p/q \in \mathbf{Q}$ distinct de a/b, on a

$$\left|\vartheta - \frac{p}{q}\right| \ge \frac{1}{bq},$$

comme on le voit en utilisant, pour l'entier $aq - bp$, la propriété qui est à la base de tout argument diophantien : *si m est un entier non nul, alors $|m| \ge 1$.*

Inversement, le lemme suivant montre que, si un nombre est irrationnel, alors il admet de bonnes approximations rationnelles.

Lemme 1.4. *Soit ϑ un nombre réel. Les conditions suivantes sont équivalentes.*
(i) *ϑ est irrationnel.*
(ii) *Pour tout $\epsilon > 0$, il existe $p/q \in \mathbf{Q}$ tel que*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}.$$

(iii) *Pour tout nombre réel $Q > 1$, il existe un entier q dans l'intervalle $1 \leq q < Q$ et un entier rationnel p tel que*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{qQ}.$$

(iv) *Il existe une infinité de $p/q \in \mathbf{Q}$ tels que*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Démonstration. Les implications (iii)⇒(iv)⇒(ii)⇒(i) du lemme 1.4 sont faciles. Il ne reste qu'à démontrer (i)⇒(iii), qui est un théorème de Dirichlet. Pour l'établir nous allons utiliser le principe des tiroirs.

Soit Q un nombre réel > 1. On pose $N = \lceil Q \rceil$: autrement dit N est l'entier déterminé par $N - 1 < Q \leq N$. Comme $Q > 1$, on a $N \geq 2$.

Soit $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$. On considère le sous-ensemble E de l'intervalle unité $[0, 1]$ constitué des $N + 1$ éléments

$$0,\ \{\vartheta\},\ \{2\vartheta\},\ \{3\vartheta\},\ \ldots, \{(N-1)\vartheta\},\ 1.$$

Comme ϑ est irrationnel, ces $N + 1$ éléments sont deux-à-deux distincts. On découpe l'intervalle $[0, 1]$ en N intervalles

$$I_j = \left[\frac{j}{N}\,,\, \frac{j+1}{N}\right] \quad (0 \leq j \leq N-1).$$

D'après le principe des tiroirs de Dirichlet, un au moins de ces N intervalles, disons I_{j_0}, contient au moins deux éléments de E. À part 0 et 1, les éléments $\{q\vartheta\}$ de E avec $1 \leq q \leq N - 1$ sont irrationnels, donc appartiennent à la réunion des intervalles *ouverts* $(j/N,\ (j + 1)/N)$ avec $0 \leq j \leq N - 1$.

Si $j_0 = N - 1$, alors l'intervalle

$$I_{j_0} = I_{N-1} = \left[1 - \frac{1}{N}\ ;\ 1\right]$$

contient 1 ainsi qu'un autre élément de E de la forme $\{q\vartheta\}$avec $1 \leq q \leq N-1$. On pose $p = [q\vartheta]+1$. Alors on a $1 \leq q \leq N - 1 < Q$ et

$$p - q\vartheta = [q\vartheta] + 1 - [q\vartheta] - \{q\vartheta\} = 1 - \{q\vartheta\}, \quad \text{donc} \quad 0 < p - q\vartheta < \frac{1}{N} \leq \frac{1}{Q}.$$

Sinon on a $0 \leq j_0 \leq N-2$ et I_{j_0} contient deux éléments $\{q_1\vartheta\}$ and $\{q_2\vartheta\}$ avec $0 \leq q_1 < q_2 \leq N-1$. On pose

$$q = q_2 - q_1, \quad p = [q_2\vartheta] - [q_1\vartheta].$$

Ainsi on a $0 < q = q_2 - q_1 \leq N - 1 < Q$ et

$$|q\vartheta - p| = |\{q_2\vartheta\} - \{\, q_1\vartheta\}| < 1/N \leq 1/Q.$$

□

Exercice. Soient $x_1, \ldots, x_m$ des nombres réels. Les propriétés suivantes sont équivalentes.
(i) Un au moins des nombres $x_1, \ldots, x_m$ est irrationel.
(ii) Pour tout $\epsilon > 0$, il existe $p_1, \ldots, p_m, q$ dans $\mathbf{Z}$ avec $q > 0$ tel que

$$0 < \max_{1 \le i \le m} \left| x_i - \frac{p_i}{q} \right| < \frac{\epsilon}{q}.$$

(iii) Pour tout entier $Q > 1$, il existe $p_1, \ldots, p_m, q$ dans $\mathbf{Z}$ tel que $1 \le q \le Q^m$ et

$$0 < \max_{1 \le i \le m} \left| x_i - \frac{p_i}{q} \right| \le \frac{1}{qQ}.$$

(iv) L'ensemble des $q \in \mathbf{Z}$, $q > 0$, pour lesquels il existe $p_1, \ldots, p_m$ dans $\mathbf{Z}$ satisfaisant

$$0 < \max_{1 \le i \le m} \left| x_i - \frac{p_i}{q} \right| < \frac{1}{q^{1+1/m}},$$

est infini.
`Indication.` Pour la démonstration de (i)⇒(iii), on pourra utiliser le principe des tiroirs de Dirichlet : considérer les $Q^m + 1$ éléments

$$\xi_q = \big(\{qx_1\}, \ldots, \{qx_m\}\big) \quad (q = 0, 1, \ldots, Q^m)$$

dans le cube unité $[0,1)^m$ de $\mathbf{R}^m$ et découper ce cube unité en Q^m cubes dont les côtés ont pour longueur $1/Q$.

Il y a d'autres démonstrations de (i)⇒(iii). Par exemple on peut utiliser un théorème de Minkowski en géométrie des nombres ; cela permet de démontrer des variantes du lemme 1.4. En particulier en dimension supérieure le principe des tiroirs donne des énoncés moins précis que la géométrie des nombres.

Une autre variante de la démonstration du théorème de Dirichlet (implication (i)⇒(iii) du lemme 1.4) repose sur les suites de Farey : la *suite de Farey d'indice n* est constituée par la suite croissante des nombres rationnels de l'intervalle unité dont le dénominateur est $\le n$. Par exemple la suite de Farey d'indice 6 est

$$0,\ \frac{1}{6},\ \frac{1}{5},\ \frac{1}{4},\ \frac{1}{3},\ \frac{2}{5},\ \frac{1}{2},\ \frac{3}{5},\ \frac{2}{3},\ \frac{3}{4},\ \frac{4}{5},\ \frac{5}{6},\ 1.$$

On peut montrer (cf [13], Ch. I § 2, Th. 2.A) que deux fractions consécutives $p/q < r/s$ d'une suite de Farey satisfont $qr - ps = 1$. Il en résulte que si

$$\frac{p}{q} < \frac{u}{v} < \frac{r}{s}$$

sont trois fractions consécutives d'une suite de Farey, alors

$$\frac{u}{v} = \frac{p+r}{q+s}.$$

Cela résulte des relations $qu - pv = 1$ et $vr - us = 1$.

L'implication (i)⇒(iv) du lemme 1.4 peut être améliorée :

Lemme 1.5 (Hurwitz)**.** *Soit ϑ un nombre réel. Les propriétés suivantes sont équivalentes.*
(i) *ϑ est irrationnel.*
(ii) *Il existe une infinité de $p/q \in \mathbf{Q}$ satisfaisant*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Évidemment l'implication (ii)⇒(i) du lemme 1.5 est une forme affaiblie de l'implication (iv)⇒(i) du lemme 1.4. Ce qui est nouveau est la réciproque.

Les démonstrations classiques de l'équivalence entre les assertions (i) et (ii) du lemme 1.5 font intervenir soit les fractions continues, soit les suites de Farey. Même si les fractions continues n'interviennent pas explicitement dans la démonstration qui suit, elles sont sous-jacentes.

Lemme 1.6. *Soit ϑ un nombre réel irrationnel. Il existe une infinité de couples $(p/q, r/s)$ de fractions rationnelles irréductibles telles que*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad et \quad qr - ps = 1.$$

Dans cet énoncé et les deux suivants, il suffit de démontrer les inégalités larges $\leq$ à la place des inégalités strictes $<$ grâce à l'hypothèse que ϑ est irrationnel.

Démonstration. Soit H un entier positif. Parmi les fractions rationnelles irréductibles a/b avec $1 \leq b \leq H$, on en choisit une pour laquelle $|\vartheta - a/b|$ est minimal. Si $a/b < \vartheta$ on appelle p/q cette fraction a/b, tandis que si $a/b > \vartheta$, alors on l'appelle r/s.

Commençons par le cas où $a/b < \vartheta$, donc $a/b = p/q$. Comme $\mathrm{pgcd}(p, q) = 1$, l'algorithme d'Euclide (théorème de Bézout) montre qu'il existe $(r, s) \in \mathbf{Z}^2$ tel que $qr - ps = 1$ avec $1 \leq s < q$ et $|r| < |p|$. De $1 \leq s < q \leq H$, en rappelant le choix de a/b, on déduit

$$\left|\vartheta - \frac{p}{q}\right| \leq \left|\vartheta - \frac{r}{s}\right|$$

donc r/s n'est pas dans l'intervalle $[p/q, \vartheta]$. Mais $qr - ps > 0$, donc $p/q < r/s$, par conséquent $\vartheta < r/s$.

Dans le second cas où $a/b > \vartheta$ et $r/s = a/b$ on résout $qr - ps = 1$ par l'algorithme d'Euclide avec $1 \leq q < s$ et $|p| < r$. On conclut de la même manière.

Il reste à montrer qu'on obtient une infinité de tels couples de rationnels. Une fois qu'on dispose d'un ensemble fini de couples $(p/q, r/s)$, on utilise le fait qu'il existe un nombre rationnel m/n qui est plus proche de ϑ que chacune de ces fractions de l'ensemble fini (c'est la densité de $\mathbf{Q}$ dans $\mathbf{R}$). On reprend l'argument précédent avec un entier $H > n$. Cela permet de construire un couple $(p/q, r/s)$ de nombres rationnels qui est différent des précédents, puisque l'une au moins des nouvelles approximations p/q ou r/s est meilleure que les précédentes. Donc cette construction fournit une infinité de couples. □

Lemme 1.7. *Soit ϑ un nombre réel irrationnel. Soient $(p/q, r/s)$ deux fractions irréductibles telles que*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad et \quad qr - ps = 1.$$

Alors

$$\min\left\{q^2\left(\vartheta-\frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s}-\vartheta\right)\right\}<\frac{1}{2}.$$

Démonstration. Posons

$$\delta=\min\left\{q^2\left(\vartheta-\frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s}-\vartheta\right)\right\}.$$

En ajoutant les inégalités

$$\frac{\delta}{q^2}\le\vartheta-\frac{p}{q}\quad\text{et}\quad\frac{\delta}{s^2}\le\frac{r}{s}-\vartheta$$

et en utilisant $qr-ps=1$, on déduit que le nombre $t=s/q$ satisfait

$$t+\frac{1}{t}\le\frac{1}{\delta}.$$

Comme le minimum de la fonction $t\mapsto t+1/t$ est 2 et comme $t\neq1$, on en déduit $\delta<1/2$.

□

Remarque. La minoration $t+(1/t)\ge2$ pour tout $t>0$, qui est stricte pour $t\neq1$, est équivalente à l'inégalité arithmético-géométrique

$$\sqrt{xy}\le\frac{x+y}{2},$$

pour x et y nombres réels positifs, avec égalité si et seulement si if $x=y$. La correspondance entre les deux énoncés se fait en posant $t=\sqrt{x/y}$.

Des lemmes 1.6 et 1.7 on déduit que pour tout $\vartheta\in\mathbf{R}\setminus\mathbf{Q}$, il existe une infinité de $p/q\in\mathbf{Q}$ satisfaisant

$$0<\left|\vartheta-\frac{p}{q}\right|<\frac{1}{2q^2}.$$

Il faut encore un pas de plus pour compléter la démonstration du lemme 1.5.

Lemme 1.8. *Soit ϑ un nombre irrationnel. On suppose que $(p/q,r/s)$ sont deux fractions irréductibles telles que*

$$\frac{p}{q}<\vartheta<\frac{r}{s}\quad\textit{et}\quad qr-ps=1.$$

On pose $u=p+r$ et $v=q+s$. Alors

$$\min\left\{q^2\left(\vartheta-\frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s}-\vartheta\right)\ ,\ v^2\left|\vartheta-\frac{u}{v}\right|\right\}<\frac{1}{\sqrt{5}}.$$

Démonstration. Notons déjà que $qu-pv=1$ et $rv-su=1$. Donc

$$\frac{p}{q}<\frac{u}{v}<\frac{r}{s}.$$

On répète la démonstration du lemme 1.7 ; on distingue deux cas selon que u/v est supérieur ou inférieur à ϑ. Comme les deux cas se traitent de la même manière, supposons $\vartheta<u/v$. La démonstration du lemme 1.7 montre que

$$\frac{s}{q}+\frac{q}{s}\le\frac{1}{\delta}\quad\text{et}\quad\frac{v}{q}+\frac{q}{v}\le\frac{1}{\delta}.$$

Donc chacun des quatre nombres s/q, q/s, v/q, q/v satisfait $t+1/t \le 1/\delta$. La fonction $t \mapsto t+1/t$ est décroissante sur l'intervalle $(0,1)$ et croissante sur l'intervalle $(1,+\infty)$. Il en résulte que nos quatre nombres sont dans l'intervalle $(1/x, x)$, où x est la racine >1 de l'équation $x+1/x = 1/\delta$. Les deux racines x et $1/x$ du polynôme quadratique $X^2 - (1/\delta)X + 1$ ont pour distance la racine carrée du discriminant $\Delta = (1/\delta)^2 - 4$ de ce polynôme. Comme

$$\frac{v}{q} - \frac{s}{q} = 1,$$

il en résulte que la longueur $\sqrt{\Delta}$ de l'intervalle $(1/x, x)$ est ≥ 1. Par conséquent $\Delta \ge 1$ et $\delta \le 1/\sqrt{5}$. Ceci termine la démonstration du lemme 1.8. □

Montrons que le lemme 1.5 est optimal. Désignons par

$$\Phi = \frac{1+\sqrt{5}}{2} = 1.618\,033\,988\,749\,9\ldots$$

le nombre d'or, qui est la racine >1 du polynôme $X^2 - X - 1$. Le discriminant de ce polynôme est 5.

Lemme 1.9. *Pour tout $q \ge 1$ et tout $p \in \mathbf{Z}$,*

$$\left|\Phi - \frac{p}{q}\right| > \frac{1}{\sqrt{5}q^2 + (1/\sqrt{5})}.$$

Démonstration. Il suffit d'établir la minoration quand

$$\left|\Phi - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

On factorise le polynôme $X^2 - X - 1 = (X - \Phi)(X + \Phi^{-1})$. Ainsi

$$p^2 - pq - q^2 = q^2 \left(\frac{p}{q} - \Phi\right)\left(\frac{p}{q} + \Phi^{-1}\right).$$

Le membre de gauche est un entier rationnel non nul, sa valeur absolue est donc au moins 1. Majorons maintenant la valeur absolue du membre de droite. Comme

$$p < q\Phi + (1/\sqrt{5}q) \quad \text{et} \quad \Phi + \Phi^{-1} = \sqrt{5},$$

on a

$$\frac{p}{q} + \Phi^{-1} \le \sqrt{5} + \frac{1}{\sqrt{5}q^2}.$$

Donc

$$1 \le q^2 \left|\frac{p}{q} - \Phi\right| \left(\sqrt{5} + \frac{1}{\sqrt{5}q^2}\right).$$

Le lemme 1.9 en résulte.

□

Pour le nombre d'or on peut exhiber la suite des meilleures approximations rationnelles. Pour cela on considère la suite de Fibonacci $(F_n)_{n\geq 0}$ définie par :

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

Lemme 1.10. *On a*

$$\lim_{n\to\infty} F_{n-1}^2 \left|\Phi - \frac{F_n}{F_{n-1}}\right| = \frac{1}{\sqrt{5}}.$$

Démonstration. L'espace vectoriel formé par les suites $(v_n)_{n\geq 0}$ qui satisfont $v_n = v_{n-1} + v_{n-2}$ a pour dimension 2, une base étant donnée par les deux suites $(\Phi^n)_{n\geq 0}$ et $((-\Phi^{-1})^n)_{n\geq 0}$. La formule

$$F_n = \frac{1}{\sqrt{5}}(\Phi^n - (-1)^n\Phi^{-n}),$$

due à A. De Moivre (1730), L. Euler (1765) et J.P.M. Binet (1843) en résulte. Par conséquent F_n est l'entier le plus proche de

$$\frac{1}{\sqrt{5}}\Phi^n,$$

donc la suite $(u_n)_{n\geq 2}$ des quotients consécutifs de nombres de Fibonacci

$$u_n = F_n/F_{n-1}$$

vérifie $\lim_{n\to\infty} u_n = \Phi$.

Par récurrence on vérifie

$$F_n^2 - F_nF_{n-1} - F_{n-1}^2 = (-1)^{n-1}$$

pour $n \geq 1$. Le membre de gauche est $F_{n-1}^2(u_n - \Phi)(u_n + \Phi^{-1})$, comme nous l'avons déjà vu. Donc

$$F_{n-1}^2|\Phi - u_n| = \frac{1}{\Phi^{-1} + u_n},$$

et la limite du membre de droite est $1/(\Phi + \Phi^{-1}) = 1/\sqrt{5}$. Le lemme 1.10 est ainsi démontré. □

Remarque. La suite $u_n = F_n/F_{n-1}$ est aussi définie par

$$u_2 = 2,\ u_n = 1 + \frac{1}{u_{n-1}}, \quad (n \geq 3).$$

Donc

$$u_n = 1 + \frac{1}{1 + \dfrac{1}{u_{n-2}}} = 1 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{u_{n-3}}}} = \cdots = 1 + \frac{1\ |}{|1+}\ \frac{1\ |}{|1+}\ \cdots\ + \frac{1\ |}{|1+}\ \frac{1|}{|1}.$$

Partant d'un rectangle de côtés 1 et 2, si on construit par récurrence des rectangles de plus en plus grands en ajoutant au rectangle précédent un carré posé sur le grand côté, la suite des longueurs des côtés de ces carrés est la suite de Fibonacci. C'est la construction inverse de celle qui donne le développement en fraction continue du nombre d'or, consistant à découper un rectangle dont les proportions sont données par le nombre d'or en un carré plus un rectangle plus petit ayant de nouveau le nombre d'or comme proportions.

Exercice. a) Soit $f(X,Y) = aX^2 + bXY + cY^2 \in \mathbf{R}[X,Y]$ un polynôme homogène de degré 2 à coefficients réels de discriminant positif

$$\Delta = b^2 - 4ac > 0.$$

Soit $\epsilon > 0$. Montrer qu'il existe $(x,y) \in \mathbf{Z}^2$ avec $(x,y) \neq (0,0)$ tel que

$$|f(x,y)| \leq \sqrt{\Delta/5} + \epsilon.$$

b) Soit Δ un nombre réel positif. Donner un exemple d'un polynôme homogène f de degré 2 dont le discriminant est Δ tel que

$$\min\big\{|f(x,y)| \; ; \; (x,y) \in \mathbf{Z} \times \mathbf{Z}, \; (x,y) \neq (0,0)\big\} = \sqrt{\Delta/5}.$$

c) Soit Δ un nombre réel positif. Donner un exemple d'un polynôme homogène $f(X,Y) = aX^2 + bXY + cY^2$ de degré 2 dont le discriminant $b^2 - 4ac$ est Δ et tel que

$$\min\big\{|f(x,y)| \; ; \; (x,y) \in \mathbf{Z} \times \mathbf{Z}, \; (x,y) \neq (0,0)\big\} = \sqrt{\Delta/8}.$$

d) Donner un exemple d'un polynôme homogène f de degré 2 de discriminant $\Delta > 0$ tel que

$$\min\big\{|f(x,y)| \; ; \; (x,y) \in \mathbf{Z} \times \mathbf{Z}, \; (x,y) \neq (0,0)\big\} = 0.$$

Si α est racine d'un polynôme quadratique $P(X) = aX^2 + bX + c$, alors $P'(\alpha) = 2a\alpha + b$ est une racine carrée du discriminant de P. D'après le lemme 1.9, le lemme de Hurwitz 1.5 est optimal pour toutes les racines de polynômes quadratiques de discriminant 5. En passant, cela montre que 5 est le plus petit discriminant d'un polynôme quadratique irréductible de $\mathbf{Z}[X]$ (évidemment on vérifie de façon élémentaire que si a, b, c sont trois entiers rationnels satisfaisant $a > 0$ et $b^2 - 4ac$ positif sans être un carré parfait dans $\mathbf{Z}$, alors $b^2 - 4ac \geq 5$).

Soit x un nombre réel irrationnel. Désignons par $\gamma(x) \in [\sqrt{5}, +\infty]$ la borne supérieure des nombres réels $\gamma > 0$ tels qu'il existe une infinité de $p/q \in \mathbf{Q}$ satisfaisant

$$\left|x - \frac{p}{q}\right| \leq \frac{1}{\gamma q^2}.$$

La minoration $\gamma \geq \sqrt{5}$ n'est autre que le lemme 1.5 de Hurwitz. Les lemmes 1.5 et 1.9 montrent que $\gamma(\Phi) = \sqrt{5}$.

En écrivant

$$\left|x + 1 - \frac{p}{q}\right| = \left|x - \frac{p+q}{q}\right| \quad \text{et} \quad \left|-x - \frac{p}{q}\right| = \left|x + \frac{p}{q}\right|,$$

on obtient $\gamma(x+1) = \gamma(-x) = \gamma(x)$. On montre aussi que $\gamma(1/x) = \gamma(x)$. Il en résulte que si x et y sont deux nombres réels que l'on déduit l'un de l'autre en itérant ces trois opérations $x \mapsto x+1$, $x \mapsto -x$ et $x \mapsto 1/x$, alors $\gamma(x) = \gamma(y)$. Un résultat classique ([14] Chap. VII § 1.2) est que le groupe multiplicatif engendré par les trois matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

est le groupe des matrices 2×2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

à coefficients dans $\mathbf{Z}$ de déterminant ± 1. Nous n'allons pas utiliser cet énoncé mais nous démontrons directement :

Lemme 1.11. *Soit $x \in \mathbf{R} \setminus \mathbf{Q}$ et soient a, b, c, d des entiers rationnels satisfaisant $ad - bc = \pm 1$. On pose*

$$y = \frac{ax+b}{cx+d}.$$

Alors $\gamma(x) = \gamma(y)$.

Démonstration. Soit $\epsilon > 0$ et soit $\gamma = \gamma(x) - \epsilon$. Par définition de $\gamma(x)$, existe une infinité de $p/q \in \mathbf{Q}$ tels que

$$\left| x - \frac{p}{q} \right| \le \frac{1}{\gamma q^2}.$$

Comme c et d ne sont pas tous deux nuls, au plus un d'entre eux satisfait $cp+dq = 0$. On s'intéresse aux autres. Posons

$$r = ap + bq, \quad s = cp + dq.$$

Quitte à changer les signes de a, b, c et d on peut supposer $s > 0$. On écrit

$$y - \frac{r}{s} = \frac{ax+b}{cx+d} - \frac{ap+bq}{cp+dq} = \frac{(ad-bc)(qx-p)}{(cx+d)(cp+dq)} = \pm \frac{qx-p}{(cx+d)(cp+dq)}$$

et

$$\left| y - \frac{r}{s} \right| \le \frac{1}{\gamma q} \cdot \left| \frac{1}{(cx+d)(cp+dq)} \right| = \frac{1}{\gamma s^2} \cdot \frac{cp+dq}{q|cx+d|}.$$

Pour q suffisamment grand on a

$$|c| \cdot \left| x - \frac{p}{q} \right| \le \frac{|c|}{\gamma q^2} \le \epsilon |cx+d|,$$

donc

$$\left| \frac{cp+dq}{q(cx+d)} - 1 \right| \le \epsilon$$

et

$$\left| y - \frac{r}{s} \right| \le \frac{1+\epsilon}{\gamma s^2}.$$

Comme il y a une infinité de $r/s \in \mathbf{Q}$ satisfaisant cette inégalité on en déduit

$$\gamma(y) \ge \frac{\gamma}{1+\epsilon} = \frac{\gamma(x) - \epsilon}{1+\epsilon}.$$

Cette inégalité est vraie pour tout $\epsilon > 0$, par conséquent $\gamma(y) \ge \gamma(x)$. Comme

$$x = \frac{-dy+b}{cy-a},$$

en permutant x et y on obtient l'égalité annoncée $\gamma(y) = \gamma(x)$. □

Des lemmes 1.5, 1.9 et 1.11 on déduit que tous les nombres réels x de la forme $(a\Phi+b)/(c\Phi+d)$ avec a, b, c, d dans $\mathbf{Z}$ et $ad-bc=\pm1$ satisfont $\gamma(x)=\sqrt{5}$. Hurwitz a aussi montré que pour tous les autres nombres réels irrationnels y, on a $\gamma(y)\geq 2\sqrt{2}$. Cette inégalité est optimale, comme on le voit en prenant $y=\sqrt{2}$ (voir la formule (1.12) dans l'exercice ci-dessous). Le lemme 1.11 implique alors $\gamma(y)=2\sqrt{2}$ pour tout y de la forme $(a\sqrt{2}+b)/(c\sqrt{2}+d)$ avec $ad-bc=\pm1$, et une fois de plus la minoration peut être améliorée pour tous les autres nombres réels irrationnels. Ce processus donne lieu à une suite d'exposants

$$\sqrt{5},\sqrt{8},\sqrt{221}/5,\sqrt{1517}/13,\dots$$

convergeant vers 1/3, qui est à l'origine de l'équation de Markoff (0.5) (cf [3] Chap. 7).

Remarque. Les développements en fraction continue des nombres quadratiques qui apparaissent dans cette suite ne font apparaître que des 1 et des 2. On sait (voir par exemple [13] p. 25) que si k est un entier positif, si le développement en fraction continue $[a_0;a_1,a_2,\dots]$ d'un nombre réel irrationnel ϑ satisfait $a_n\geq k$ pour une infinité de n, alors

$$\liminf_{q\to\infty} q^2\left|\vartheta-\frac{p}{q}\right|\leq\frac{1}{\sqrt{4+k^2}}\cdot$$

Exercice. On pose $G_0=0$, $G_1=1$, et par récurrence on définit $G_n=2G_{n-1}+G_{n-2}$ pour $n\geq 2$.
a) Vérifier, pour tout $n\geq 1$,

$$G_n^2-2G_nG_{n-1}-G_{n-1}^2=(-1)^{n-1}.$$

b) Montrer que la suite $(G_n/G_{n-1})_{n\geq2}$ converge quand $n\to\infty$. Quelle est la limite ?
c) Montrer qu'il existe une suite $(p_n/q_n)_{n\geq1}$ de nombre rationnels telle que

$$\lim_{n\to\infty} q_n\left|q_n\sqrt{2}-p_n\right|=\frac{1}{2\sqrt{2}}\cdot \tag{1.12}$$

d) Montrer que pour tout $\kappa>2\sqrt{2}$, il n'y a qu'un nombre fini de nombres rationnels $p/q\in\mathbf{Q}$ satisfaisant

$$\left|\sqrt{2}-\frac{p}{q}\right|\leq\frac{1}{\kappa q^2}\cdot$$

Remarque. Partant plus généralement d'une suite récurrente linéaire $u_{n+1}=au_n+bu_{n-1}$ où a et b sont deux entiers rationnels, si on pose $v_n=u_n^2-au_nu_{n-1}-bu_{n-1}^2$, on vérifie par récurrence $v_n=(-b)^nv_0$.

1.3 Nombres : algébriques, transcendants

Un nombre complexe qui est racine d'un polynôme non nul à coefficients rationnels est appelé *algébrique*. Ainsi les nombres rationnels (racines d'un polynôme de degré 1) sont algébriques, $\sqrt{2}$ et i, racines des polynômes X^2-2 et X^2+1 sont algébriques irrationnels – on les appelle *quadratiques* car ils sont racines de polynômes de degré 2. Un nombre *cubique* est une racine d'un polynôme de degré 3 ; un exemple est $\sqrt[3]{2}$.

Étant donné un nombre algébrique α, l'ensemble des polynômes à coefficients rationnels qui s'annulent en α forme un idéal premier de $\mathbf{Q}[X]$, cet idéal est principal, chacun de ses générateurs

est un polynôme irréductible de $\mathbf{Q}[X]$ dont le degré est le *degré de* α. Il y a un unique générateur unitaire, qui est appelé **le** *polynôme irréductible* de α. Quand on multiplie ce polynôme par le ppcm des dénominateurs de ses coefficients, on obtient le *polynôme minimal* de α, qui est l'unique polynôme irréductible dans l'anneau *factoriel* $\mathbf{Z}[X]$ s'annulant au point α et ayant un coefficient directeur positif. Voir par exemple [9] Chap. 2 § 5 pour les prérequis concernant notamment les anneaux factoriels.

Les nombres algébriques complexes forment un corps. L'exercice suivant en fournit une démonstration.

Exercice. a) Soient x un nombre complexe et n un entier positif. Montrer que les conditions suivantes sont équivalentes.
(i) Le nombre x est racine d'un polynôme non nul de $\mathbf{Q}[X]$ de degré $\leq n$.
(ii) Les nombres $1, x, x^2, \ldots, x^n$ sont linéairement dépendants sur $\mathbf{Q}$.
(iii) Le $\mathbf{Q}$–espace vectoriel engendré par les nombres x^i, $(i \geq 1)$ est de dimension $\leq n$.
b) Montrer que l'inverse $1/x$ d'un nombre algébrique non nul x est un nombre algébrique.
c) Soient x et y deux nombres algébriques. Montrer que le $\mathbf{Q}$–espace vectoriel engendré par $x^i y^j$, $(i \geq 0,\ j \geq 0)$ est de dimension finie. En déduire que le produit de deux nombres algébriques est un nombre algébrique.
d) Soient x et y deux nombres algébriques. Montrer que le $\mathbf{Q}$–espace vectoriel engendré par $x^i + y^j$, $(i \geq 0,\ j \geq 0)$ est de dimension finie. En déduire que la somme de deux nombres algébriques est un nombre algébrique.

Un nombre complexe est dit *transcendant* s'il n'est pas algébrique. L'ensemble des nombres transcendants ne jouit pas de bonnes propriétés algébriques : la somme de nombres transcendants peut être un nombre rationnel, ou algébrique irrationnel, ou encore transcendant. De même pour le produit de deux nombres transcendants. La somme d'un nombre algébrique et d'un nombre transcendant est un nombre transcendant. Le produit d'un nombre algébrique *non nul* et d'un nombre est un nombre transcendant. La racine carrée (et plus généralement la racine k-ième, pour $k \geq 1$) d'un nombre transcendant est un nombre transcendant. Toute puissance entière ≥ 1 d'un nombre transcendant est encore un nombre transcendant.

L'existence de nombres transcendants a été établie en 1844 par J. Liouville. Son idée consiste à établir une propriété satisfaite par tous les nombres algébriques, puis à exhiber des nombres qui ne satisfont pas cette propriété. Ce que montre Liouville est que les nombres algébriques irrationnels sont relativement mal approchés par des nombres rationnels.

Le lemme suivant ([13] p. 6 Lemma 2E) est une des nombreuses variantes de l'inégalité de Liouville. On peut le voir comme un généralisation du lemme 1.10 : au lieu de $X^2 - X - 1$ on prend n'importe quel polynôme irréductible de degré ≥ 2, ce qui revient à remplacer le nombre d'or par n'importe quel nombre algébrique irrationnel.

Lemme 1.13. *Soit α un nombre algébrique racine de degré $d \geq 2$ et soit $P \in \mathbf{Z}[X]$ son polynôme minimal. On pose $c = |P'(\alpha)|$. Soit $\epsilon > 0$. Alors il existe un entier q_0 tel que, pour tout $p/q \in \mathbf{Q}$ avec $q \geq q_0$, on ait*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(c+\epsilon)q^d}.$$

Démonstration. Soit q un entier suffisamment grand et soit p l'entier le plus proche de $q\alpha$. En particulier on a

$$|q\alpha - p| \leq \frac{1}{2}.$$

On désigne par a_0 le coefficient directeur de P (quitte à remplacer s'il le faut P par $-P$, on supposera $a_0 > 0$) et par $\alpha_1, \ldots, \alpha_d$ ses racines, avec $\alpha_1 = \alpha$. Ainsi

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_d)$$

et

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^{d} \left(\frac{p}{q} - \alpha_i\right). \tag{1.14}$$

On a aussi

$$P'(\alpha) = a_0 \prod_{i=2}^{d} (\alpha - \alpha_i).$$

Le membre de gauche de (1.14) est un entier rationnel car P est de degré d à coefficients entiers. Il n'est pas nul parce que P est irréductible de degré ≥ 2. Pour $i \geq 2$ on a

$$\left|\alpha_i - \frac{p}{q}\right| \leq |\alpha_i - \alpha| + \frac{1}{2q}\cdot$$

On déduit de (1.14)

$$1 \leq q^d a_0 \left|\alpha - \frac{p}{q}\right| \prod_{i=2}^{d} (|\alpha_i - \alpha| + \frac{1}{2q}).$$

Pour q suffisamment grand le membre de droite est majoré par

$$q^d \left|\alpha - \frac{p}{q}\right| (|P'(\alpha)| + \epsilon).$$

□

Le corollaire suivant du lemme 1.13 est le résultat principal de J. Liouville en 1844 : c'est l'outil qui lui a permis, non seulement de montrer l'existence de nombres transcendants, mais aussi d'en exhiber. Ses premiers exemples utilisaient des fractions continues (1.1). Ensuite il a utilisé des séries rapidement convergentes comme

$$\vartheta = \sum_{n \geq 0} g^{-n!}$$

pour tout entier $g \geq 2$.

Lemme 1.15. *Pour tout nombre algébrique α, il existe une constante $\kappa > 0$ telle que, pour tout nombre rationnel $p/q \neq \alpha$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{\kappa q^d},$$

où d est le degré de α

Démonstration. Quand $d = 1$ ce résultat est vrai en prenant pour κ le dénominateur de α. Supposons maintenant $d \geq 2$. Le lemme 1.13 avec $\epsilon = 1$ montre que l'inégalité est vraie avec $\kappa = c + 1$

pour q suffisamment grand, disons $q \geq q_0$. Pour avoir un résultat uniforme (pour tout p/q) il suffit de prendre

$$\kappa = \max\left\{c+1, \max_{1\leq q<q_0} \frac{1}{q^{d-1}|q\alpha - p|}\right\}.$$

□

Exercice. Le lemme 1.15 est trivial si α n'est pas réel. Dire pourquoi.

Exercice. On désigne par $P \in \mathbf{Z}[X]$ le polynôme minimal de α, par a_0 son coefficient directeur et par $\alpha_1, \ldots, \alpha_d$ ses racines, avec $\alpha_1 = \alpha$:

$$P(X) = a_0(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_d).$$

a) Démontrer le lemme 1.15 avec

$$\kappa = \max\{1\ ;\ \max_{|t-\alpha|\leq 1} |P'(t)|\}.$$

b) Démontrer le lemme 1.15 avec

$$\kappa = a_0 \prod_{i=2}^{d} (|\alpha_j - \alpha| + 1).$$

`Indication` *Pour les deux parties de l'exercice, on pourra distinguer deux cas selon que* $|\alpha - (p/q)|$ *est* ≥ 1 *ou* < 1.

Exercice. a) Soit θ un nombre réel dans l'intervalle $0 < \theta < 3$. Montrer que les deux propriétés suivantes sont équivalentes.
(i) Il existe une constante $c_1 > 0$ telle que, pour tout nombre rationnel p/q, on ait

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{c_1}{q^\theta}.$$

(ii) Il existe une constante $c_2 > 0$ telle que, pour tout couple (x, y) d'entiers $\neq (0, 0)$, on ait

$$|x^3 - 2y^3| \geq c_2 |y|^{3-\theta}.$$

b) Montrer qu'il existe une constante $c_3 > 0$ telle que, pour une infinité de couple (x, y) d'entiers, on ait

$$|x^3 - 2y^3| \leq c_3 |y|.$$

Définition. Un nombre réel ϑ est un *nombre de Liouville* si, pour tout $\kappa > 0$, il existe $p/q \in \mathbf{Q}$ avec $q \geq 2$ tel que

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^\kappa}.$$

Le lemme 1.15 implique que les nombres de Liouville sont transcendants [1]. Dans la théorie des systèmes dynamiques, on dit qu'un nombre réel *satisfait une condition Diophantienne* si ce n'est pas un nombre de Liouville : cela signifie qu'il existe une constante $\kappa > 0$ telle que, pour tout $p/q \in \mathbf{Q}$ avec q suffisamment grand,

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^\kappa}.$$

`Exemple.` Soit $g \geq 2$ un entier rationnel et soit $(a_n)_{n\geq 0}$ une suite bornée d'entiers rationnels. On suppose qu'une infinité d'entre eux ne sont pas nuls. Montrons que *le nombre*

$$\vartheta = \sum_{n\geq 0} a_n g^{-n!}$$

est un nombre de Liouville.

Soit $A = \max_{n\geq 0} |a_n|$ et soit $\kappa > 0$ un nombre réel. Prenons pour N un entier suffisamment grand avec $a_{N+1} \neq 0$ et posons

$$q = g^{N!}, \quad p = \sum_{n=0}^{N} a_n g^{N!-n!}.$$

On a $p \in \mathbf{Z}$, $q \in \mathbf{Z}$, $q > 0$ et

$$\vartheta - \frac{p}{q} = \frac{a_{N+1}}{g^{(N+1)!}} + \sum_{k\geq 2} \frac{a_{N+k}}{g^{(N+k)!}}.$$

Pour $k \geq 2$ on utilise l'estimation grossière

$$(N+k)! - (N+1)! \geq N + k$$

qui donne, pour N suffisamment grand,

$$\sum_{k\geq 2} \frac{|a_{N+k}|}{g^{(N+k)!}} \leq \frac{A}{g^{(N+1)!}} \sum_{k\geq 2} \frac{1}{g^{N+k}} < \frac{1}{g^{(N+1)!}} \leq \frac{|a_{N+1}|}{g^{(N+1)!}},$$

donc $\vartheta \neq p/q$ et

$$0 < \left|\vartheta - \frac{p}{q}\right| \leq \frac{2|a_{N+1}|}{g^{(N+1)!}}.$$

On utilise enfin $|a_{N+1}| \leq A$ et $g^{(N+1)!} = q^{N+1}$, d'où

$$0 < \left|\vartheta - \frac{p}{q}\right| \leq \frac{2A}{q^{N+1}}.$$

Il en résulte que ϑ est un nombre de Liouville.

Après que Liouville ait construit les premiers exemples de nombres transcendants, G. Cantor a donné un autre argument qui montre non seulement qu'il existe des nombres transcendants, mais aussi qu'il y en a *beaucoup*. La première étape consiste à montrer que les nombres algébriques forment un ensemble dénombrable. Pour cela il remarque que pour chaque couple (d, H) d'entiers

[1] `Exercice : rédiger la démonstration de cette affirmation.`

positifs, il n'y a qu'un nombre fini de polynômes à coefficients entiers de degré $\leq d$ dont tous les coefficients ont une valeur absolue $\leq H$, et chacun de ces polynômes n'a qu'un nombre fini de racines. La réunion de l'ensemble de ces racines, quand d et H varient, est une réunion dénombrable d'ensembles dénombrables, donc est dénombrable, et c'est l'ensemble des nombres algébriques.

Pour obtenir l'existence de nombres transcendants, Cantor introduit son *argument diagonal* : si on numérote les nombres algébriques de l'intervalle $(0,1)$ et qu'on écrit chacun d'eux avec son développement en base 2 (en prenant soin d'écrire les deux développements pour les quotients d'un entier par une puissance de 2, l'un qui termine par des 0, l'autre qui termine par des 1), disons

$$\begin{array}{rcl} x_1 & = & 0, a_{11}\, a_{12}\, a_{13} \cdots a_{1n} \cdots \\ x_2 & = & 0, a_{21}\, a_{22}\, a_{33} \cdots a_{2n} \cdots \\ x_3 & = & 0, a_{31}\, a_{32}\, a_{33} \cdots a_{3n} \cdots \\ & \vdots & \\ x_m & = & 0, a_{m1}\, a_{m2}\, a_{m3} \cdots a_{mn} \cdots \\ & \vdots & \end{array}$$

et si on pose $b_n = 1 - a_{nn}$, alors le nombre réel

$$y = 0, b_1 b_2 b_3 \cdots b_n \cdots$$

n'est pas dans la liste, puisqu'il diffère de x_n au moins par le n-ième chiffre ; il est donc transcendant.

Cette construction donne aussi la transcendance du nombre

$$z = 0, a_{11} a_{22} a_{33} \cdots a_{nn} \cdots ,$$

puisque $y + z = 1$.

On sait (voir par exemple l'appendice 1 de [9] ou bien le chapitre 12 de [6]) que le nombre e est transcendant (Hermite, 1873), que le nombre π est transcendant (Lindemann, 1882). Plus généralement le théorème de Hermite–Lindemann s'énonce sous les deux formes équivalentes suivantes.

Théorème 1.16 (Hermite–Lindemann)**.** *a) Soit α un nombre algébrique non nul et soit $\log\alpha$ un logarithme non nul de α (c'est-à-dire un nombre complexe tel que $\exp(\log\alpha) = \alpha$). Alors $\log\alpha$ est un nombre transcendant.*
b) Soit β un nombre algébrique non nul. Alors le nombre e^β est transcendant.

Exercice. Vérifier que les deux énoncés a) et b) du théorème 1.16 sont bien équivalents.

En 1934, A.O. Gel'fond et Th. Schneider ont résolu le 7ème des 23 problèmes posés par D. Hilbert en 1900. On peut de nouveau énoncer ce résultat sous deux formes équivalentes.

Théorème 1.17 (Gel'fond–Schneider)**.** *a) Soient α un nombre algébrique non nul, β un nombre algébrique irrationnel et $\log\alpha$ un logarithme non nul de α. Alors le nombre α^β, qui est défini comme $\exp(\beta\log\alpha)$, est transcendant.*
b) Soient α_1 et α_2 deux nombres algébriques non nuls, $\log\alpha$ et $\log\alpha_2$ des logarithmes non nuls de α_1 et α_2 respectivement. On suppose que le quotient $\log\alpha_1/\log\alpha_2$ est irrationnel. Alors $\log\alpha_1/\log\alpha_2$ est transcendant.

Exercice. Vérifier que les deux énoncés a) et b) du théorème 1.17 sont bien équivalents.

Exercice. Déduire du théorème 1.17 la transcendance de chacun des nombres

$$2^{\sqrt{2}}, \quad 2^i, \quad e^\pi, \quad e^{\pi\sqrt{2}}, \quad \cos(\pi\sqrt{2}), \quad \frac{\log 3}{\log 2}, \quad \frac{\pi}{\log 2}.$$

Exercice. On considère un nombre complexe non nul a, un nombre complexe irrationnel b, et une détermination non nulle $\log a$ du logarithme de a. Chacun des trois nombres a, b et $a^b = e^{b \log a}$ peut être algébrique ou transcendant, ce qui fait a priori 8 possibilités, mais le théorème de Gel'fond–Schneider montre que l'une de ces possibilités est exclue : les trois nombres en question ne peuvent pas tous être algébriques. Donner un exemple de chacune des 7 autres situations (on pourra utiliser les théorèmes de Hermite–Lindemann et Gel'fond–Schneider).