Université P. et M. Curie (Paris VI),
Deuxième semestre 2007/2008

Michel Waldschmidt

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

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Deuxième fascicule : 21/01/2008

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

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

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 [2] 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

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

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

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

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.

$\square$

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.
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 $(2N)!/2^{N-m}(2m)!$ $(0 \leq m \leq N)$ 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

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

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.
d) Montrer que le nombre $e^{\sqrt{3}}$ est irrationnel.
e) Soit $(a_n)_{n\geq 0}$ 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 $n \geq N_0$.
(ii) Le nombre

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

est rationnel
(iii) Le nombre

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

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

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

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 $|m| \geq 1$.*

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*

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

(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*

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

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

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

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

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

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 $\vartheta_1, \ldots, \vartheta_m$ des nombres réels. Les propriétés suivantes sont équivalentes.
(i) Un au moins des nombres $\vartheta_1, \ldots, \vartheta_m$ est irrationel.
(ii) Pour tout $\epsilon > 0$, il existe $p_1, \ldots, p_m, q$ dans $\mathbf{Z}$ avec $q > 0$ tel que

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

(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

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

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

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

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

$$\xi_q = \big(\{q\vartheta_1\}, \ldots, \{q\vartheta_m\}\big) \quad (q = 0, 1, \ldots, Q^m)$$

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 [2], 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

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

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*

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

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 algébrique irrationnel. Il existe une infinité de couples $(p/q, r/s)$ de fractions rationnelles irréductibles telles que*

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

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*

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

Alors

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

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

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

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

Remarque. La minoration $t+(1/t)\ge 2$ pour tout $t>0$, qui est stricte pour $t\neq 1$, 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

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

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

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

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

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

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

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

Donc chacun des quatre nombres s/q, q/s, v/q, q/v satisfait $t + 1/t \leq 1/\delta$. 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 $\Delta \geq 1$ et $\delta \leq 1/\sqrt{5}$. Ceci termine la démonstration du lemme 1.8. □

Montrons que le lemme 1.5 est optimal. Désignons par $\Phi = 1.6180339887499\ldots$ 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 $q \geq 1$ et tout $p \in \mathbf{Z}$,*

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

Démonstration. Il suffit d'établir la minoration quand p est l'entier le plus proche de $q\Phi$. 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 $p < q\Phi + (1/2)$ et $\Phi + \Phi^{-1} = \sqrt{5}$ on a

$$\frac{p}{q} + \Phi^{-1} \leq \sqrt{5} + \frac{1}{2q} \cdot$$

Donc

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

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*

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

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

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

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

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

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

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

Références

[1] J.H. Conway & R.K. Guy – *The book of numbers*, Copernicus Books, Springer Science + Business Media, 2006.

[2] W. M. Schmidt – *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer-Verlag, Berlin, 1980.