Indépendance linéaire de certains nombres algébriques

(Ces rśultats vous sont offerts par David A. Madore)

Le but de ce papier est de démontrer et d'appliquer le très grand et très profond théorème suivant.

Théorème super génial. *La famille $(\sqrt{m})$, où m parcourt l'ensemble des naturels sans facteur carré, est linéairement libre sur $\mathbb{Q}$.*

On va démontrer par récurrence sur n la proposition suivante :

Proposition. *Si $p_1, \ldots, p_n$ sont des naturels distincts de 1, deux à deux étrangers et sans facteur carré, alors les 2^n réels*

$$1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1 p_2}, \ldots, \sqrt{p_1 \cdots p_n}$$

sont linéairement indépendants sur $\mathbb{Q}$.

La proposition est évidente pour $n = 0$. Elle est bien connue pour $n = 1$ (c'est ici qu'on utilise le fait que les p_i sont distincts de 1), et elle était du reste connue de Pythagore au sixième siècle avant notre ère ; par acquis de conscience, nous allons cependant la redémontrer.

Supposons donc $s_0 + s_1\sqrt{p_1} = 0$ avec s_0, s_1 rationnels, p_1 naturel distinct de 1 sans facteur carré. On veut montrer $s_0 = s_1 = 0$. On peut clairement supposer s_0, s_1 entiers. Supposons par l'absurde s_0, s_1 non tous deux nuls. Quitte à diviser par un diviseur commun, on peut supposer s_0, s_1 étrangers. On a alors $s_0^2 = p_1 s_1^2$. Mais ceci montre que s_0^2 est divisible par p_1, et donc, comme p_1 est sans facteur carré, que s_0 l'est aussi ; dans ce cas, on peut écrire $s_0 = p_1 t$ avec t entier. Alors $s_0^2 = p_1^2 t^2$ donc $s_1^2 = p_1 t^2$, donc p_1 divise s_1^2, donc aussi s_1. Et comme p_1 n'est pas égal à 1, et qu'il divise s_0 et s_1, ceux-ci ne sont pas étrangers, contradiction.

Supposons maintenant la proposition vraie au rang $n - 1$, avec $n \geq 2$, et montrons qu'elle est vraie au rang n.

Considérons pour cela les nombres de la forme

$$r_{0\cdots0} + r_{0\cdots01}\sqrt{p_1} + \cdots + r_{1\cdots1}\sqrt{p_1 \cdots p_{n-1}} \qquad (*)$$

où $r_{0\cdots0}, \ldots, r_{1\cdots1}$ sont rationnels. Il est manifeste que ces nombres forment une algèbre commutative K de dimension finie* sur $\mathbb{Q}$. De plus, cette algèbre est clairement intègre. Or une algèbre intègre de dimension finie est un corps (en effet, la multiplication à gauche par un élément non nul est linéaire et injective, donc bijective, donc atteint 1). Par suite, les nombres de la forme $(*)$ forment un *corps commutatif*, qui n'est bien entendu autre que

$$K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{n-1}})$$

D'après l'hypothèse de récurrence, les coefficients qui interviennent dans l'écriture $(*)$ sont uniquement déterminés. Si nous appelons L le corps $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-2}})$ (naturellement, si $n = 2$, on prend $L = \mathbb{Q}$), alors tout élément de K s'écrit de façon unique sous la forme $a + b\sqrt{p_{n-1}}$, avec $a, b \in L$.

Supposons maintenant que l'on ait

$$s_{0\cdots0} + s_{0\cdots01}\sqrt{p_1} + \cdots + s_{1\cdots1}\sqrt{p_1 \cdots p_n} = 0 \qquad (**)$$

et nous allons montrer que $s_{0\cdots0} = \cdots = s_{1\cdots1} = 0$. On constate que $(**)$ peut encore s'écrire

$$s_0 + s_1\sqrt{p_n} = 0$$

avec $s_0, s_1 \in K$, précisément

$$s_0 = s_{0\cdots0} + s_{0\cdots01}\sqrt{p_1} + \cdots + s_{01\cdots1}\sqrt{p_1 \cdots p_{n-1}}$$

et

$$s_1 = s_{10\cdots0} + s_{10\cdots01}\sqrt{p_1} + \cdots + s_{1\cdots1}\sqrt{p_1 \cdots p_{n-1}}$$

D'après l'hypothèse de récurrence, montrer que $s_{0\cdots0} = \cdots = s_{1\cdots1} = 0$ équivaut à montrer que $s_0 = 0$ et $s_1 = 0$. Supposons par l'absurde que s_1 est non nul. Alors on a

$$\sqrt{p_n} = -\frac{s_0}{s_1}$$

* Cette dimension est $\leq 2^{n-1}$; d'après l'hypothèse de récurrence, c'est même exactement 2^{n-1}, mais nous n'avons pas encore utilisé l'hypothèse de récurrence.

donc $\sqrt{p_n} \in K$. On peut alors écrire $\sqrt{p_n} = a + b\sqrt{p_{n-1}}$ et $a, b \in L$. Mais alors $p_n = (a^2 + p_{n-1}b^2) + 2ab\sqrt{p_{n-1}}$, et comme on a vu que l'écriture d'un élément de K sous la forme $a' + b'\sqrt{p_{n-1}}$ avec $a', b' \in L$ est unique, on en tire

$$\begin{cases} a^2 + p_{n-1}b^2 = p_n \\ ab = 0 \end{cases}$$

De $ab = 0$ on tire soit $b = 0$ soit $a = 0$. Dans le premier cas, $a^2 = p_n$, et nous posons $x = a$, $p = p_n$; dans le second cas, $(p_{n-1}b)^2 = p_{n-1}p_n$, et nous posons $x = p_{n-1}b$, $p = p_{n-1}p_n$. On a ainsi $x^2 = p$ dans tous les cas, où $x \in L$ et p est un entier sans facteur carré (c'est ici qu'on utilise l'hypothèse que les p_i sont étrangers deux à deux) étranger à $p_1, \ldots, p_{n-2}$. De cela, on tire immédiatement $\sqrt{p} \in L$, et donc $\sqrt{p}$ est combinaison linéaire de $1, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_1 \cdots p_{n-2}}$. Mais ceci contredit l'hypothèse de récurrence appliquée à $p_1, \ldots, p_{n-2}, p$. C'est donc que l'hypothèse $s_1 \neq 0$ est absurde, et donc $s_1 = 0$ et donc aussi $s_0 = 0$. Ceci termine la récurrence.

Le théorème lui-même est maintenant pratiquement évident : si $m_1, \ldots, m_k$ sont des naturels sans facteur carré, soient $p_1, \ldots, p_n$ les nombres premiers qui divisent l'un des m_j. Alors les m_j se trouvent tous parmi les nombres

$$1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1p_2}, \ldots, \sqrt{p_1 \cdots p_n}$$

(c'est ici qu'on utilise le fait que les m_j sont sans facteur carré) ; ils sont donc linéairement indépendants sur $\mathbb{Q}$, ce qui démontre le théorème.

A titre d'exemple d'utilisation du théorème, on a le

Corollaire-exemple. *Pour tout naturel $n > 1$, la somme*

$$\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}}$$

n'est pas un rationnel.

En effet, pour tout rationnel r, $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} - r$ s'écrit comme une combinaison linéaire à coefficients rationnels de nombres de la forme $\sqrt{m}$ où m est sans facteur carré (il suffit pour le voir de faire passer les racines au numérateur et de sortir les facteurs carrés des racines). Reste seulement à voir que tous les coefficients de cette combinaison linéaire sont non nuls. Mais c'est clair car le coefficient de $\sqrt{2}$ est $1 + \frac{1}{2} + \cdots + \frac{1}{k}$ (pour un certain k) et n'est donc certainement pas nul.

Le théorème montre de manière semblable l'irrationnalité de $\sqrt{2} + \cdots + \sqrt{n}$, ou de $\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}} + \cdots + \frac{(-1)^n}{\sqrt{n}}$, ou de $\sqrt{2} - \sqrt{3} + \cdots + (-1)^n\sqrt{n}$. En revanche, le résultat suivant est plus subtil :

Corollaire. *Pour tout naturel $n > 1$, et tous rationnels $\alpha_2, \ldots, \alpha_n$ non nuls, la somme*

$$\alpha_2\sqrt{2} + \alpha_3\sqrt{3} + \cdots + \alpha_n\sqrt{n}$$

n'est pas un rationnel.

Encore une fois, il faut voir qu'un des coefficients de la combinaison linéaire obtenue comme précédemment est non nul. Pour cela, soit m le plus grand entier inférieur ou égal à n et sans facteur carré. Le nombre de multiples de 4 dans $]\frac{n}{4}; n]$ est inférieur strictement à $\frac{1}{4}(n - \frac{n}{4}) + 1$, le nombre de multiples de 9, inférieur strictement à $\frac{1}{9}(n - \frac{n}{4}) + 1$, et ainsi de suite. Le nombre d'entiers de $]\frac{n}{4}; n]$ ayant un facteur carré est donc inférieur strictement à $(\frac{\pi^2}{6} - 1)(n - \frac{n}{4}) + \sqrt{n}$. Par ailleurs, le nombre d'entiers dans $]\frac{n}{4}; n]$ est supérieur ou égal à $n - \frac{n}{4}$. Ainsi, le nombre d'entiers sans facteur carré dans $]\frac{n}{4}; n]$ est supérieur strictement à $\frac{3}{4}(2 - \frac{\pi^2}{6})n - \sqrt{n}$, et pour $n \geq (\frac{4}{3(2-\pi^2/6)})^2$, soit en fait $n \geq 15$, il y a un entier sans facteur carré dans $]\frac{n}{4}; n]$, et en particulier, $m > \frac{n}{4}$. Pour $n \leq 14$, l'assertion est également vraie comme on le vérifie immédiatement "à la main". De plus, on a $m > 1$. Mais $m > \frac{n}{4}$ signifie encore $4m > n$, et par conséquent, le seul terme mettant en jeu $\sqrt{m}$ est $\alpha_m\sqrt{m}$ lui-même. Par conséquent, le coefficient de $\sqrt{m}$ est non nul. Ceci montre le corollaire.