Sur les sommes de racines

Daniel PERRIN

L'objectif de ce texte est de montrer qu'une somme de racines d'entiers positifs ne peut être rationnelle que si tous sont des carrés parfaits [1], voir 2.3. Au passage on précisera la structure des extensions de $\mathbf{Q}$ obtenues en lui adjoignant un nombre fini de racines d'entiers positifs.

1 Préliminaires

On commence par quelques remarques :

1.1 *Remarques.* 1) Soit $a \in \mathbf{N}$ non nul. Si a est un carré de $\mathbf{Q}$ c'est un carré de $\mathbf{N}$. En effet, si $a = \dfrac{p^2}{q^2}$ avec p, q premiers entre eux, on a $q^2 a = p^2$ et le théorème de Gauss donne le résultat. Bien entendu, c'est le fait que $\mathbf{Z}$ est intégralement clos.

2) Si K est un corps et si a et b sont dans K^*, il revient au même de dire que ab ou b/a est un carré dans K (car on a $ab = (b/a) \times a^2$).

Vu 1.1.1, le lemme suivant est évident :

1.2 Lemme. *1) Soit K un corps et soit $a \in K$. L'extension $K(\sqrt{a})$ est de degré 1 (resp. 2) si a est un carré de K (resp. sinon).*

2) Soit a un entier > 0. Si a est un carré parfait dans $\mathbf{N}$ on a $\mathbf{Q}(\sqrt{a}) = \mathbf{Q}$ et sinon $\mathbf{Q}(\sqrt{a})$ est de dimension 2 sur $\mathbf{Q}$.

On a ensuite une caractérisation des carrés dans une extension quadratique :

1.3 Lemme. *Soit K un corps et $a \in K$ un élément non carré. Un élément $b \in K$ est un carré dans $K(\sqrt{a})$ si et seulement si b ou ab est un carré de K.*

Démonstration. On écrit $b = (x + y\sqrt{a})^2$ avec $x, y \in K$ et on a $b = x^2 + ay^2 + 2xy\sqrt{a}$. Comme b est dans K on a $xy = 0$ donc $x = 0$ ou $y = 0$. Si y est nul, b est un carré de K, si c'est x, on a $b = ay^2$ et b/a (ou ab) est un carré de K.

1. Je remercie Pierre Lecomte de m'avoir posé cette belle question.

Enfin on a une première approche des extensions engendrées par des racines carrées :

1.4 Lemme. *Soient $a_1, \ldots, a_n$ des entiers > 0. Le corps $L := \mathbf{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ est engendré comme $\mathbf{Q}$-espace vectoriel par les éléments $\sqrt{a_{i_1} \cdots a_{i_k}}$ avec $0 \leq k \leq n$ et $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. Il est donc de dimension $\leq 2^n$ sur $\mathbf{Q}$.*

Démonstration. On raisonne par récurrence sur n. Le cas $n = 1$ est donné par 1.2. Pour passer de $n-1$ à n on note que si l'on a des extensions $K \subset L \subset M$, si $e_1, \ldots, e_p$ engendrent L sur K et $f_1, \ldots, f_q$ engendrent M sur L, les $e_i f_j$ engendrent M sur K.

2 Le résultat principal

2.1 Théorème. *Soient $a_1, \ldots, a_n$ des entiers positifs. Les conditions suivantes sont équivalentes :*

1) Le corps $L := \mathbf{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ est de dimension 2^n sur $\mathbf{Q}$.

2) Les nombres $a_1, \ldots, a_n$ sont linéairement indépendants dans $\mathbf{Q}^*/\mathbf{Q}^{*2}$ vu comme espace vectoriel sur le corps à 2 éléments.

3) Aucun des nombres a_i, $a_i a_j$, $a_i a_j a_k$, $\ldots$, $a_1 \cdots a_n$ n'est un carré parfait.

Si ces conditions sont réalisées, une base de L sur $\mathbf{Q}$ est formée des $\sqrt{a_{i_1} \cdots a_{i_k}}$ avec $0 \leq k \leq n$ et $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. L'extension L est galoisienne sur $\mathbf{Q}$ et son groupe de Galois est $(\mathbf{Z}/2\mathbf{Z})^n$. Les extensions de degré 2 contenues dans L sont exactement les $\mathbf{Q}(\sqrt{a_{i_1} \cdots a_{i_k}})$ pour $k \geq 1$.

Démonstration. Une relation de dépendance linéaire dans $\mathbf{Q}^*/\mathbf{Q}^{*2}$ est de la forme $a_1^{\lambda_1} \cdots a_n^{\lambda_n} \in \mathbf{Q}^{*2}$ avec des λ_i égaux à 0 ou 1. Une relation non triviale exprime donc le fait que $a_{i_1} \cdots a_{i_k}$ est un carré de $\mathbf{Q}$, donc de $\mathbf{N}$, ce qui montre l'équivalence des conditions 2) et 3).

Le fait que L est engendré comme $\mathbf{Q}$-espace vectoriel par les $\sqrt{a_{i_1} \cdots a_{i_k}}$ (voir 1.4) montre que 1) implique 3).

Il reste à montrer 3) $\Longrightarrow$ 1). On raisonne par récurrence sur n, le cas $n = 1$ résultant de 1.2. L'hypothèse de récurrence appliquée à $n-1$ dit que $K := \mathbf{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-1}})$ est de degré 2^{n-1} et, par multiplicativité des degrés, il suffit de voir que $\sqrt{a_n}$ n'est pas dans K. Sinon, par Galois et l'hypothèse de récurrence, il serait dans une des extensions de degré 2, $\mathbf{Q}(\sqrt{a_{i_1} \cdots a_{i_k}})$ avec $1 \leq i_1 < \ldots < i_k \leq n-1$ et, comme a_n n'est pas un carré, cela impose que $a_{i_1} \cdots a_{i_k} a_n$ en est un en vertu de 1.3 et c'est absurde.

La famille des $\sqrt{a_{i_1} \cdots a_{i_k}}$ étant génératrice et du bon cardinal est une base. L'extension est galoisienne car c'est le corps de décomposition du polynôme $(X^2 - a_1) \cdots (X^2 - a_n)$. Si $(\epsilon_1, \ldots, \epsilon_n)$ est un élément de $\{-1, 1\}^n$, il

est clair [2] que l'on obtient un automorphisme de L sur $\mathbf{Q}$ en posant $\sigma(\sqrt{a_i}) = \epsilon_i\sqrt{a_i}$, de sorte que le groupe de Galois contient $\{-1,1\}^n \simeq (\mathbf{Z}/2\mathbf{Z})^n$ et il lui est égal pour une raison de cardinal. Par la théorie de Galois, les extensions de degré 2 contenues dans L correspondent aux sous-groupes d'indice 2 de $(\mathbf{Z}/2\mathbf{Z})^n$, c'est-à-dire aux hyperplans. Leur nombre est égal au nombre de formes linéaires non nulles donc à 2^n-1. Ces extensions sont donc exactement les 2^n-1 citées.

2.2 Corollaire. *Soient $a_1,\dots,a_n$ des entiers positifs et $L := \mathbf{Q}(\sqrt{a_1},\dots,\sqrt{a_n})$. Le degré de L sur $\mathbf{Q}$ est de la forme 2^r avec $r \leq n$ et il existe r entiers $a_{i_1},\dots,a_{i_r}$ parmi $a_1,\dots,a_n$ qui vérifient les conditions du théorème 2.1 et dont les racines engendrent L.*

Démonstration. C'est évident en choisissant parmi les a_i une base du sous-espace vectoriel qu'ils engendrent dans $\mathbf{Q}^*/\mathbf{Q}^{*2}$.

2.3 Corollaire. *Soient $a_1,\dots,a_n$ des entiers positifs. Alors, $\sqrt{a_1}+\cdots+\sqrt{a_n}$ est rationnel si et seulement si tous les a_i sont des carrés parfaits.*

Démonstration. On raisonne par l'absurde. Soit $L = \mathbf{Q}(\sqrt{a_1},\dots,\sqrt{a_n})$. Comme tous les a_i ne sont pas des carrés parfaits, ce corps n'est pas égal à $\mathbf{Q}$. Comme il est engendré par les $\sqrt{a_{i_1}\cdots a_{i_k}}$, la relation $\sqrt{a_1}+\cdots+\sqrt{a_n}-s=0$ avec $s\in\mathbf{Q}$ montre qu'il est de dimension $< 2^n$. En vertu de 2.2, et quitte à renuméroter les a_i, on peut supposer qu'il existe $r \leq n-1$ tel que l'on ait $L = \mathbf{Q}(\sqrt{a_1},\dots,\sqrt{a_r})$ où $a_1,\dots,a_r$ vérifient les hypothèses du théorème 2.1.

Mais alors, la théorie de Galois et le lemme 1.3 impliquent que tous les a_i pour $i > r$ sont de la forme $a_{i_1}\cdots a_{i_k}u_i^2$ avec $1 \leq i_p \leq r$ et $u_i \in \mathbf{N}^*$ et l'hypothèse s'écrit sous la forme $\sqrt{a_1}+\cdots+\sqrt{a_r}+\sum_i \sqrt{a_{i_1}\cdots a_{i_k}}u_i \in \mathbf{Q}$, ce qui contredit le fait que les racines des produits des a_i pour $i \leq r$ forment une base de L sur $\mathbf{Q}$ (la relation est non triviale car les u_i sont positifs).

2.4 *Remarque.* Il n'est pas tout à fait évident de traduire la condition 3) de 2.1 en termes de factorisation des a_i. On peut supposer que les a_i sont sans facteur carré sans changer l'extension et donc que chaque a_i est produit de nombres premiers distincts. Un moyen de tester si $a_1,\dots,a_n$ vérifient 3) est le suivant. On appelle P l'ensemble des nombres premiers intervenant dans les a_i et on note N son cardinal. On peut alors écrire, pour tout i, $a_i = \prod_{p\in P} p^{\epsilon_{p,i}}$ avec $\epsilon_{p,i}$ égal à 0 ou 1. On considère l'espace vectoriel de dimension 2^n sur $\mathbf{F}_2$ dont une base correspond aux produits $a_{i_1}\cdots a_{i_k}$ (et qui n'est autre que l'ensemble V des parties de $\{1,2,\dots,n\}$) et l'application $\mathbf{F}_2$-linéaire qui à un élément $A\in V$ associe l'élément $(\epsilon_p)_{(p\in P)}$ de $\mathbf{F}_2^N$ défini par $\epsilon_p := \sum_{i\in A}\epsilon_{p,i}$. Alors, l'élément $\prod_{i\in A} a_i$ est un carré si et seulement si on a $\Phi(A)=0$.

2. Voir par exemple Perrin, *Cours d'algèbre*, Ch. III, lemme 1.31.

Il en résulte que la condition pour que 3) soit vérifiée c'est que Φ soit injective ou encore que son noyau soit nul.

Quand on a explicitement les a_i on est ramené à un problème matriciel sur $\mathbf{F}_2$ que l'on peut aisément traiter avec un logiciel de calcul formel même dans le cas de données de grande taille.

2.5 *Exemple.* Si l'on a $a = 2 \times 3 \times 7 \times 11$, $b = 3 \times 5 \times 11$ et $c = 2 \times 5 \times 7$, l'application Φ a pour matrice la transposée de $\begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$ et on vérifie que le vecteur $(1, 1, 1)$ est dans le noyau de Φ, ce qui signifie que abc est un carré.

2.6 *Remarque.* Une condition suffisante pour avoir la condition 3) est que les ensembles A_i supports des a_i (c'est-à-dire $A_i = \{p \mid \epsilon_{p,i} = 1\}$) soient non vides et deux à deux disjoints. Mais cette condition n'est évidemment pas nécessaire comme le montre l'exemple de $a = pq$, $b = qr$ et $c = r$.