An. Şt. Univ. Ovidius Constanţa Vol. 19(2), 2011, 15–36

# THE IRRATIONALITY OF SUMS OF RADICALS VIA COGALOIS THEORY

**Toma Albu**

**Abstract**

In this paper we present an one-and-a-half-line proof, involving Cogalois Theory, of a folklore result asking when is an irrational number a sum of radicals of positive rational numbers. Some of the main ingredients of Cogalois Theory like $G$-Kneser extension, $G$-Cogalois extension, etc., used in the proof are briefly explained, so that the paper is self-contained. We also discuss some older and newer results on transcendental and irrational numbers.

## Introduction

The aim of this paper is three-fold: firstly, to discuss various aspects related to transcendental and irrational numbers, including presentation of some open questions on this matter, secondly, to present in this context a folklore result asking when is a sum of radicals of positive rational numbers an irrational number, with an one-and-a-half-line proof via Cogalois Theory, and thirdly, to shortly explain those notions and facts of this theory used in that proof. Finally, a few applications of Cogalois Theory, including an extension of the folklore result from $\mathbb{Q}$ to any subfield of $\mathbb{R}$, mainly answering some problems discussed in the paper, are presented.

Key Words: Irrational number, algebraic number, transcendental number, field extension, Galois extension, radical extension, Kummer extension, Cogalois Theory, Kneser extension, Cogalois extension, $G$-Cogalois extension, elementary Field Arithmetic.
Mathematics Subject Classification: 11J72, 11J81, 12-02, 12E30, 12F05.

Note that the first two sections are of a very elementary level, being addressed to anybody wishing to be acquainted with older as well as newer results on transcendental and irrational numbers. The last two sections require, however, some knowledge of Field Theory, including the Fundamental Theorem of Galois Theory.

## 1 Transcendental and irrational numbers

In this section we present some more or less known results on transcendental and irrational numbers, including those related to the irrationality of $\zeta(n)$ and of the Euler's constant.

By $\mathbb{N}$ we denote the set $\{0, 1, 2, \ldots\}$ of all natural numbers, and by $\mathbb{Z}$ (resp. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) the set of all rational integers, (resp. rational, real, complex) numbers. For any $\varnothing \neq A \subseteq \mathbb{C}$ (resp. $\varnothing \neq X \subseteq \mathbb{R}$) we denote $A^* := A \setminus \{0\}$ (resp. $X_+ := \{\, x \in X \,|\, x \geqslant 0 \,\}$. If $a \in \mathbb{R}_+^*$ and $n \in \mathbb{N}^*$, then the unique positive real root of the equation $x^n - a = 0$ will be denoted by $\sqrt[n]{a}$.

**Definitions 1.1.** *An* algebraic number *is any number $a \in \mathbb{C}$ which is a root of a nonzero polynomial $f \in \mathbb{Q}[X]$, and a* transcendental number *is any number $t \in \mathbb{C}$ which is not algebraic.* □

Throughout this paper we will use the following notation:

$$\begin{aligned} \mathbb{A} &:= \text{the set of all algebraic numbers,} \\ \mathbb{T} &:= \mathbb{C} \setminus \mathbb{A} = \text{the set of all transcendental numbers,} \\ \mathbb{I} &:= \mathbb{R} \setminus \mathbb{Q} = \text{the set of all irrational numbers.} \end{aligned}$$

**Examples 1.2.** (1) $\mathbb{Q} \subseteq \mathbb{A}$ since any $a \in \mathbb{Q}$ is the root of the nonzero polynomial $f = X - a \in \mathbb{Q}[X]$.

(2) $\sqrt[n]{a} \in \mathbb{A}$ for any $a \in \mathbb{Q}_+^*$ and $n \in \mathbb{N}^*$ because there exists $f = X^n - a \in \mathbb{Q}[X]$ such that $f(\sqrt[n]{a}) = 0$.

(3) $\mathbb{T} \cap \mathbb{R} \subseteq \mathbb{I}$ since $\mathbb{Q} \subseteq \mathbb{A}$.

(4) $e := \lim\limits_{n\to\infty} \left(1 + \dfrac{1}{n}\right)^n \in \mathbb{T}$, as this has been proved by *Charles Hermite* (1822-1901) in 1873.

(5) $\pi \in \mathbb{T}$, as this has been proved by *Ferdinand von Lindemann* (1852-1939) in 1882. □

Clearly,

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I} \quad \text{and} \quad \mathbb{Q} \cap \mathbb{I} = \varnothing,$$

therefore any real number defined by certain natural procedures like geometrical constructions, limits of sequences, etc., can be either *rational* or *irrational*. Therefore it is natural to ask the following

**Problem 1.3.** *Decide whether a given real number is* rational *or* irrational. □

As we will see below this problem is in general extremely difficult. However, notice that in the real life we are dealing only with rational numbers, so the problem makes no sense in this context.

**Examples 1.4.** (1) $\sqrt{2} \in \mathbb{I}$. Notice that $\sqrt{2}$ is precisely the length of the diagonal of the square of side 1. It seems that this number, discovered by *Pitagora* ($\sim$ 570 - 495 BC) and *Euclid* ($\sim$ 300 BC), was the first ever known irrational number.

(2) $\pi \in \mathbb{I}$ because we have seen above that $\pi \in \mathbb{T}$. This number appears as the length of the circle with diameter 1. However, in the real life $\pi = 3.141$.

(3) $e := \lim\limits_{n\to\infty} \left(1 + \dfrac{1}{n}\right)^n \in \mathbb{I}$ because we have noticed above that $e \in \mathbb{T}$. However, in the real life $e = 2.718$.

(4) $\zeta(2k) \in \mathbb{I}$, $\forall\, k \in \mathbb{N}^*$, where

$$\zeta(s) := \lim_{n\to\infty}\left(\frac{1}{1^s}+\frac{1}{2^s}+\cdots+\frac{1}{n^s}\right),\ s\in\mathbb{C},\ \Re(s)>1,$$

is the famous zeta function of *Bernhard Riemann* (1826-1866). Let us mention that the well-known *Riemann's Hypothesis*, raised in 1859 and saying that the nontrivial zeroes $z$ of the function $\zeta$ have $\Re(z)=1/2$, is one of the seven Millennium's Problems.

Indeed, by a well-known result (see, e.g., Borevitch & Shafarevitch [11, Chap. V, §8, Theorem 6], one has

$$\zeta(2k)=(-1)^{k-1}\frac{(2\pi)^{2k}}{2\cdot(2k)!}\cdot B_{2k},$$

where $B_m\in\mathbb{Q}$, $m\in\mathbb{N}^*$, are the so called *Bernoulli's numbers*, introduced by *Jakob Bernoulli* (1654-1705), but published posthumously only in 1713. It is known that $B_1=-\frac{1}{2}$ and $B_{2k+1}=0$, $\forall\, k\in\mathbb{N}^*$. Thus, $\zeta(2)=\frac{\pi^2}{6}$, $\zeta(4)=\frac{\pi^4}{90}$, $\zeta(6)=\frac{\pi^6}{945}$, etc. Since $\pi\in\mathbb{I}$ and $B_{2k}\in\mathbb{Q}$ one deduces that $\zeta(2k)\in\mathbb{I}$, as desired. □

In view of Examples 1.4 (4) it is natural to ask the following:

**Question 1.5.** *What about the irrationality of* $\zeta(2k+1)$, $k\in\mathbb{N}^*$*?*

*Answer*: Up to now it is known that $\zeta(3)\in\mathbb{I}$, as this has been proved by *Roger Apéry* (1916-1994) in 1978 (see [6] and [22]). The Apéry's magnificent proof is a mix of miracle and mystery. A more simple proof is due to *Frits Beukers* [10], and an elementary very recent proof has been done by *Yuri V. Nesterenko* [21]. In 2000, *Tanguy Rivoal* [23] proved that $\zeta(2k+1)\in\mathbb{I}$ for infinitely many $k\in\mathbb{N}^*$ (see also [7]), and, one year later, *Vadim Zudilin* showed that at least one of the numbers $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ is irrational. □

One of the hardest question of Diophantine Analysis, which has not yet been settled till now, is about the irrationality of the *Euler's constant*

$$C := \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\ln n\right)\sim 0.27721$$

considered by *Leonhard Euler* (1707-1783) in 1735, that is:

**Question 1.6.** *Is the Euler's constant irrational?*

*Answer*: It is known that in case $C \in \mathbb{Q}$ then the denominator of $C$ must be $> 10^{242,080}$. In 2009 there were known $29,844,489,545$ decimals of $C$ according to Wikipedia [25]. Let us mention that *Alexandru Froda* (1894-1973), known by an irrationality criterion [13], has claimed [14] in 1965 that his criterion can be applied to prove the irrationality of $C$; shortly after that it appeared that his claim was wrong. A more recent paper in 2003 of *Jonathan Sondow* [24] provides irrationality criteria for $C$. □

## 2 Sums of irrational numbers

In this section we discuss first the irrationality of the sum, product, and power of two irrational numbers, including $e$ and $\pi$. Then we examine when an $n$-th radical of a positive real number is irrational, and, after that, we present a nice folklore result asking when a sum of finitely many such radicals is irrational. We provide an one-and-a-half line proof of this result by invoking an important property enjoyed by the *$G$-Cogalois extension* naturally associated with the radicals intervening in the folklore result. What are these $G$-Cogalois extensions will be briefly explained in the next section.

As it is well-known, one cannot say anything about the irrationality of a sum or product of two arbitrary irrational numbers $\alpha$ and $\beta$, i.e., they can be either rational or irrational; e.g.,

$$\alpha = \sqrt{2}\,,\ \beta = -\sqrt{2} \implies \alpha + \beta = 0 \notin \mathbb{I},\ \alpha \cdot \beta = -2 \notin \mathbb{I},$$

$$\alpha = \sqrt[4]{2}\,,\ \beta = \sqrt[4]{2} \implies \alpha + \beta = 2\sqrt[4]{2} \in \mathbb{I},\ \alpha \cdot \beta = \sqrt{2} \in \mathbb{I}.$$

We have seen above that $e \in \mathbb{I}$ and $\pi \in \mathbb{I}$, so the following natural question arises:

**Question 2.1.** *What about the irrationality of* $e+\pi$ *and* $e\cdot\pi$*?*

*Answer*: It is known that *nothing is known.* □

However, a more complicated number, namely the *Gelfond's constant* $e^{\pi}\sim 23.14069$ is known to be irrational in view of the following nice result discovered independently in 1934 by *Aleksandr O. Gelfond* and *Theodor Schneider*. This result gives a positive answer to the *7th Problem* out of the 23 Problems launched by *David Hilbert* (1862-1943) at the 2nd International Congress of Mathematicians, Paris, 6 - 12 August 1900.

**Theorem 2.2.** $\alpha^{\beta}\in\mathbb{T}$, $\forall\,\alpha,\,\beta\in\mathbb{A}$, $\alpha\neq 0,\,1$, $\beta\in\mathbb{C}\setminus\mathbb{Q}$. □

Indeed, $e^{\pi}=i^{-2i}$, where, for $t,\,\alpha\in\mathbb{C}, t\neq 0$,

$$t^{\alpha}:=e^{\alpha}\ln t,\,\ln t:=\ln|t|+i\arg(z),$$

so, by Theorem 2.2, we deduce that $e^{\pi}\in\mathbb{T}$.

**Fact 2.3.** *It is not known whether* $\pi^{e}\in\mathbb{T}$. □

We are now going to examine when is an irrational number a radical of a positive real number.

*The Fundamental Theorem of Arithmetic*, FTA for short, discovered by *Euclid*, says that each natural number $a\geqslant 2$ can be uniquely written up to the order of factors as $a=p_1^{n_1}\cdot\ldots\cdot p_k^{n_k}$, with $k,\,n_1,\,\ldots,\,n_k\in\mathbb{N}^*$ and $p_1,\,\ldots,\,p_k$ distinct positive prime numbers.

As an immediate consequence of the FTA, the following *rational form* of the FTA, we abbreviate $\mathbb{Q}$-FTA, holds: every $a\in\mathbb{Q}\setminus\{0,1,-1\}$ can be uniquely written up to the order of factors as

$$a=\varepsilon\cdot p_1^{n_1}\cdot\ldots\cdot p_k^{n_k},$$

with $\varepsilon\in\{1,-1\}$, $k\in\mathbb{N}^*$, $n_1,\,\ldots,\,n_k\in\mathbb{Z}^*$, and $p_1,\,\ldots,\,p_k$ distinct positive prime numbers.

**Lemma 2.4.** *Let* $n \in \mathbb{N}$, $n \geqslant 2$, *let* $a \in \mathbb{Q}_+^*$, $a \neq 1$, *and let* $a = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$, *with* $k \in \mathbb{N}^*$, $n_1, \ldots, n_k \in \mathbb{Z}^*$, *and* $p_1, \ldots, p_k$ *distinct positive prime numbers, be the decomposition of* $a$ *given by the* $\mathbb{Q}$-FTA. *Then*

$$\sqrt[n]{a} \in \mathbb{Q} \Longleftrightarrow n \mid n_i, \forall\, i,\ 1 \leqslant i \leqslant k.$$

*Proof.* "$\Longleftarrow$": If $n \mid n_i, \forall\, i,\ 1 \leqslant i \leqslant k$, there exist $m_i \in \mathbb{N}^*$ such that $n_i = nm_i, \forall\, i,\ 1 \leqslant i \leqslant k$. We deduce that

$$\sqrt[n]{a} = \sqrt[n]{p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}} = \sqrt[n]{p_1^{nm_1} \cdot \ldots \cdot p_k^{nm_k}} = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} \in \mathbb{Q}.$$

"$\Longrightarrow$": If $b := \sqrt[n]{a} \in \mathbb{Q}$, then $b > 0$ and $b \neq 1$, so by the $\mathbb{Q}$-FTA, $b$ has a decomposition in prime factors $b = q_1^{l_1} \cdot \ldots \cdot q_s^{l_s}$, with $s \in \mathbb{N}^*$, $l_1, \ldots, l_s \in \mathbb{Z}^*$ and $q_1, \ldots, q_s$ distinct positive prime numbers. Thus

$$a = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k} = (\sqrt[n]{a})^n = b^n = (q_1^{l_1} \cdot \ldots \cdot q_s^{l_s})^n = q_1^{nl_1} \cdot \ldots \cdot q_s^{nl_s}.$$

By the uniqueness part of the $\mathbb{Q}$-FTA, we deduce that $s = k$, and by a suitable reordering of numbers $q_1, \ldots, q_s$ one has $p_i = q_i$ and $n_i = nl_i$, in other words, $n \mid n_i, \forall\, i,\ 1 \leqslant i \leqslant k$, as desired. □

**Proposition 2.5.** *Let* $n \in \mathbb{N} \setminus \{0, 1\}$ *and* $x \in \mathbb{R}_+^*$. *Then* $\sqrt[n]{x} \in \mathbb{I}$ *if and only if one and only one of the following conditions is satisfied:*

(1) $x \in \mathbb{I}$.

(2) $x \in \mathbb{Q} \setminus \{0, 1\}$ *and there exists* $i,\ 1 \leqslant i \leqslant k$, *with* $n \nmid n_i$, *where* $x = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$, $k \in \mathbb{N}^*$, $p_i$ *are distinct positive prime numbers, and* $n_i \in \mathbb{Z} \setminus \{0\}$ *for all* $i,\ 1 \leqslant i \leqslant k$.

*Proof.* Assume that $\sqrt[n]{x} \in \mathbb{I}$. There are two possibilities about $x$: either $x \in \mathbb{I}$, which is exactly condition (1), or $x \notin \mathbb{I}$. In this last case, we have neither $x = 0$ nor $x = 1$ because $\sqrt[n]{0} = 0 \in \mathbb{Q}$ and $\sqrt[1]{x} = 1 \in \mathbb{Q}$, so necessarily $x \in \mathbb{Q} \setminus \{0, 1\}$. Therefore, by the $\mathbb{Q}$-FTA, one can decompose $x$

as $x = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$, where $k \in \mathbb{N}^*$, $p_i$ are distinct positive prime numbers, and $n_i \in \mathbb{Z} \setminus \{0\}$ for all $i$, $1 \leqslant i \leqslant k$. Because $\sqrt[n]{x} \in \mathbb{I}$, by Lemma 2.4, we cannot have $n \mid n_j$, $\forall\, j$, $1 \leqslant j \leqslant k$, so there exists $i$, $1 \leqslant i \leqslant k$, with $n \nmid n_i$, as desired.

Assume that the condition (1) is satisfied, i.e., $x \in \mathbb{I}$. Then necessarily $\sqrt[n]{x} \in \mathbb{I}$, for otherwise it would follow that $x = (\sqrt[n]{x})^n \in \mathbb{Q}$, which contradicts our assumption. Assume now that the condition (2) is satisfied. By Lemma 2.4, we deduce that $\sqrt[n]{x} \in \mathbb{I}$, which finishes the proof. □

Proposition 2.5 provides a large class of irrational numbers. For instance,

$$\sqrt[4]{\frac{100}{1134}} = \sqrt[4]{\frac{2^2 \cdot 5^2}{2 \cdot 3^4 \cdot 7}} = \sqrt[4]{2^1 \cdot 3^{-4} \cdot 5^2 \cdot 7^{-1}} \in \mathbb{I}$$

because $4 \nmid 1$.

The next examples deal with the irrationality of sums of two or three square or cubic radicals of positive rational numbers, which naturally lead to ask about the general case of the irrationality of sums of finitely many $n$-th radicals of positive rational numbers.

**Examples 2.6.** (1) $\sqrt{2} + \sqrt{3} \in \mathbb{I}$. Indeed, denote $u := \sqrt{2} + \sqrt{3}$ and suppose that $u \in \mathbb{Q}$. Now, square $u - \sqrt{2} = \sqrt{3}$ to obtain $u^2 - 2u\sqrt{2} + 2 = 3$. Since $u \neq 0$, we deduce that $\sqrt{2} = \dfrac{u^2 - 1}{2u} \in \mathbb{Q}$, which is a contradiction.

(2) $\sqrt{2} + \sqrt[3]{3} \in \mathbb{I}$. Indeed, as above, denote $v := \sqrt{2} + \sqrt[3]{3}$ and suppose that $v \in \mathbb{Q}$. If we cube $v - \sqrt{2} = \sqrt[3]{3}$, we obtain $v^3 - 3\sqrt{2}\, v^2 + 6v - 2\sqrt{2} = 3$, and so $\sqrt{2} = \dfrac{v^3 + 6v - 3}{3v^2 + 2} \in \mathbb{Q}$, which is a contradiction.

(3) Similarly, with the same procedure, one can prove that for $a$, $b$, $c \in \mathbb{Q}_+^*$ the following statements hold:

$$\sqrt{a} + \sqrt{b} \in \mathbb{Q} \Longleftrightarrow \sqrt{a} \in \mathbb{Q} \ \ \& \ \ \sqrt{b} \in \mathbb{Q},$$
$$\sqrt{a} + \sqrt[3]{b} \in \mathbb{Q} \Longleftrightarrow \sqrt{a} \in \mathbb{Q} \ \ \& \ \ \sqrt[3]{b} \in \mathbb{Q},$$
$$\sqrt{a} + \sqrt{b} + \sqrt{c} \in \mathbb{Q} \Longleftrightarrow \sqrt{a} \in \mathbb{Q} \ \ \& \ \ \sqrt{b} \in \mathbb{Q} \ \ \& \ \ \sqrt{c} \in \mathbb{Q}.$$

(4) The procedure above of squaring, cubing, etc. does not work for radicals of arbitrary order, e.g., what about $\sqrt[5]{11} + \sqrt[13]{100} \in \mathbb{I}$? □

So, the following natural problem arises:

**Problem 2.7.** *When is a* sum of radicals *of form* $\sqrt[n]{a}$, $n \in \mathbb{N}^*$, $a \in \mathbb{Q}_+^*$, *a* rational/irrational *number?* □

More generally, one can ask the following

**Problem 2.8.** *Which nonempty subsets* $S \subseteq \mathbb{I}$ *have the property that any finite sum of elements of* $S$ *is again an irrational number?* □

The next result shows that

$$\mathcal{R} := \{\ \sqrt[n]{r}\ \mid\ n \in \mathbb{N},\, n \geqslant 2,\, r \in \mathbb{Q}_+^*,\, r \notin \mathbb{Q}^n\ \},$$

where $\mathbb{Q}^n = \{\, r^n \,|\, r \in \mathbb{Q}\,\}$, is such a set.

**Theorem 2.9.** (Folklore). *Let* $k, n_1, \ldots, n_k \in \mathbb{N}^*$ *and* $a_1, \ldots, a_k \in \mathbb{Q}_+^*$. *Then*

$$\sqrt[n_1]{a_1} + \cdots + \sqrt[n_k]{a_k} \in \mathbb{Q} \iff \sqrt[n_i]{a_i} \in \mathbb{Q},\ \ \forall\, i,\, 1 \leqslant i \leqslant k,$$

*or equivalently,*

$$\sqrt[n_1]{a_1} + \cdots + \sqrt[n_k]{a_k} \in \mathbb{I} \iff \exists\, i,\, 1 \leqslant i \leqslant k,\ \ \textit{such that}\ \ \sqrt[n_i]{a_i} \in \mathbb{I}.$$

The result appears explicitly as a proposed problem in 1980 by *Preda Mihăilescu*, Zürich (see [19]), a Romanian mathematician well-known for answering in positive [20] the famous *Catalan's Conjecture* raised in 1844 by *Eugène Charles Catalan* (1814-1894):

*The Diophantine equation* $x^y - z^t = 1$ *in positive integers* $x, y, z, t \geqslant 2$ *has as solutions* only *the numbers* $x = 3$, $y = 2$, $z = 2$, $t = 3$.

**Remark 2.10.** Notice that the result in Theorem 2.9 fails for $\pm$; indeed $\sqrt{12} - \sqrt{3} - \sqrt[4]{9} = 0 \in \mathbb{Q}$ but $\sqrt{12}, \sqrt{3}, \sqrt[4]{9} \in \mathbb{I}$. □

The original one-page proof of Mihăilescu [19] uses a variant of the *Vahlen-Capelli Criterion* for $\mathbb{Q}$ and includes also as reference the classical Besicovitch's paper [9]. An one-and-a-half-line proof will be given in a few moments by invoking a basic result concerning primitive elements of *G-Cogalois* extensions. What are these extensions will be shortly explained in the next section. Note that in Section 4 we will present an extension of Theorem 2.9 from $\mathbb{Q}$ to any subfield of $\mathbb{R}$, which, to the best of our knowledge, cannot be proved using the approach in [19], but only involving the tools of Cogalois Theory.

In order to present the one-and-a-half-line proof in a very elementary manner, that is accessible even at an undergraduate level, we will assign to the numbers $\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k}$ considered in the statement of Theorem 2.9, the set

$$\mathbb{Q}\,(\sqrt[n_1]{a_1}\,, \ldots, \sqrt[n_k]{a_k}\,).$$

What is this object? For short, we denote $x_i := \sqrt[n_i]{a_i} \in \mathbb{R}_+^*$, $1 \leqslant i \leqslant k$, and set

$$\mathbb{Q}^*\langle x_1\,, \ldots, x_k\rangle := \{\, a \cdot x_1^{m_1} \cdot \ldots \cdot x_k^{m_k} \mid a \in \mathbb{Q}^*,\, m_i \in \mathbb{N},\, \forall\, i, 1 \leqslant i \leqslant k\,\}.$$

Then

$$\mathbb{Q}(x_1\,, \ldots, x_k) := \{z_1 + \ldots + z_m \mid m \in \mathbb{N}^*,\, z_i \in \mathbb{Q}^*\langle x_1\,, \ldots, x_k\rangle,\, \forall\, i, 1 \leqslant i \leqslant k\,\} \cup \{0\}$$

is the set of all finite sums of elements (monomials) of $\mathbb{Q}^*\langle x_1\,, \ldots, x_k\rangle$ joined with $\{0\}$, and is in fact a subfield of the field $\mathbb{R}$. However, for the moment, the reader is not assumed to have any idea about what a field is. Observe that $\mathbb{Q}(x_1\,, \ldots, x_k) = \mathbb{Q} \Longleftrightarrow \{x_1\,, \ldots, x_k\} \subseteq \mathbb{Q}\,.$

To the best of our knowledge, there is no proof of the next result (which is a very particular case of a more general feature of $G$-Cogalois extensions), without the involvement of Cogalois Theory.

**Theorem 2.11.** (Albu & Nicolae [4]). *Let* $k, n_1, \ldots, n_k \in \mathbb{N}^*$ *and* $a_1, \ldots, a_k \in \mathbb{Q}_+^*$. *Then*

$$\mathbb{Q}\left(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k}\right) = \mathbb{Q}\left(\sqrt[n_1]{a_1} + \cdots + \sqrt[n_k]{a_k}\right). \qquad \square$$

We are now going to present the promised one-and-a-half-line proof of Theorem 2.9:

*Proof.* If $\sqrt[n_1]{a_1} + \cdots + \sqrt[n_r]{a_r} \in \mathbb{Q}$ then $\mathbb{Q}\left(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\right) = \mathbb{Q}\left(\sqrt[n_1]{a_1} + \cdots + \sqrt[n_r]{a_r}\right) = \mathbb{Q}$ by Theorem 2.11, so $\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r} \in \mathbb{Q}$. QED $\square$

## 3 Some basic concepts and facts of Cogalois Theory

In this section we will briefly explain those basic concepts and results of Cogalois Theory that have been used in proving the main result of Section 2. In contrast with the results and facts presented in the previous two sections, which can be easily understood even by a high school student, from now on, the reader is assumed to have a certain background of Field Theory, including the Fundamental Theorem of Galois Theory, at an undergraduate level.

*Cogalois Theory*, a fairly new area in Field Theory born approximately 25 years ago, investigates field extensions possessing a so called *Cogalois correspondence*. The subject is somewhat dual to the very classical *Galois Theory* dealing with field extensions possessing a *Galois correspondence*; this is the reason to use the prefix "co". In order to explain the meaning of such extensions we start with some standard notation that will be used in the sequel.

A *field extension*, for short, *extension*, is a pair $(F, E)$ of fields, where $F$ is a subfield of $E$, and in this case we write $E/F$. By an *intermediate field* of an extension $E/F$ we mean any subfield $K$ of $E$ with $F \subseteq K$, and the set of all intermediate fields of $E/F$ is a complete lattice that will be denoted by $\mathbb{I}(E/F)$.

Throughout this section $F$ always denotes a field and $\Omega$ a fixed algebraically closed field containing $F$ as a subfield. Any algebraic extension of $F$ is supposed to be a subfield of $\Omega$. For an arbitrary nonempty subset $S$ of $\Omega$ and a number $n \in \mathbb{N}^*$ we denote throughout this section $S^* := S \setminus \{0\}$ and $\mu_n(S) := \{ x \in S \mid x^n = 1 \}$. By a *primitive $n$-th root of unity* we mean any generator of the cyclic group $\mu_n(\Omega)$; $\zeta_n$ will always denote such an element. When $\Omega = \mathbb{C}$, then we can choose a canonical generator of the cyclic group $\mu_n(\mathbb{C})$ of order $n$, namely $\cos(2\pi/n) + i\sin(2\pi/n)$.

For an arbitrary group $G$, the notation $H \leqslant G$ means that $H$ is a subgroup of $G$. The lattice of all subgroups of $G$ will be denoted by $\mathbb{L}(G)$. For any subset $M$ of $G$, $\langle M \rangle$ will denote the subgroup of $G$ generated by $M$. For any set $S$, $|S|$ will denote the cardinal number of $S$.

For a field extension $E/F$ we denote by $[E : F]$ the *degree*, and by $\mathrm{Gal}\,(E/F)$ the *Galois group* of $E/F$. If $E/F$ is an extension and $A \subseteq E$, we denote by $F(A)$ the smallest subfield of $E$ containing both $A$ and $F$ as subsets, called the subfield of $E$ obtained by adjoining to $F$ the set $A$. For all other undefined terms and notation concerning basic Field Theory the reader is referred to Bourbaki [12], Karpilovsky [16], and/or Lang [18].

In general, $\mathbb{I}(E/F)$ is a complicated-to-conceive, potentially infinite set of hard-to-describe-and-identify objects, so, an interesting but difficult problem in Field Theory naturally arises:

**Problem 3.1.** *Describe in a satisfactory manner the set $\mathbb{I}(E/F)$ of all intermediate fields of a given extension $E/F$.* □

Another important problem in Field Theory is the following one:

**Problem 3.2.** *Effectively calculate the* degree *of a given extension $E/F$.* □

Answers to these two Problems are given for particular field extensions by *Galois Theory*, invented by *Évariste Galois* (1811-1832), and by *Kummer*

*Theory* invented by *Ernst Kummer* (1810-1893). We briefly recall the solution offered by Galois Theory in answering the two problems presented above.

**The Fundamental Theorem of Galois Theory (FTGT).** *If $E/F$ is a finite Galois extension with Galois group $\Gamma$, then the canonical map*

$$\alpha : \mathbb{I}(E/F) \longrightarrow \mathbb{L}(\Gamma),\ \ \alpha(K) = \mathrm{Gal}(E/K),$$

*is a lattice anti-isomorphism, i.e., a bijective order-reversing map. Moreover,* $[E : F] = |\Gamma|$. □

Thus, Galois Theory reduces the investigation of intermediate fields of a finite Galois extension $E/F$ to the investigation of subgroups of its Galois group $\mathrm{Gal}(E/F)$, which are far more benign objects than intermediate fields.

But, the Galois group of a given finite Galois extension $E/F$ is in general difficult to be concretely described. So, it will be desirable to impose additional conditions on the extension $E/F$ such that the lattice $\mathbb{I}(E/F)$ be isomorphic (or anti-isomorphic) to the lattice $\mathbb{L}(\Delta)$ of all subgroups of some other group $\Delta$, easily computable and appearing explicitly in the data of the given Galois extension $E/F$. A class of such Galois extensions is that of *classical Kummer extensions*, for which a so called *Kummer Theory*, including the *Fundamental Theorem of Kummer Theory* (FTKT) has been invented. We will not discuss them here.

On the other hand, there is an abundance of field extensions which are not necessarily Galois, but enjoy a property similar to that in FTKT or is dual to that in FTGT. These are the extensions $E/F$ possessing a canonical lattice isomorphism (and *not* a lattice anti-isomorphism as in the Galois case) between $\mathbb{I}(E/F)$ and $\mathbb{L}(\Delta)$, where $\Delta$ is a certain group canonically associated with the extension $E/F$. We call them *extensions with $\Delta$-Cogalois correspondence*. Their prototype is the field extension

$$\mathbb{Q}\left(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\right)/\mathbb{Q},$$

where $r, n_1, \ldots, n_r \in \mathbb{N}^*$, $a_1, \ldots, a_r \in \mathbb{Q}_+^*$ and $\sqrt[n_i]{a_i}$ is the positive real $n_i$-th root of $a_i$ for each $i$, $1 \leqslant i \leqslant r$. For such an extension, the associated group $\Delta$ is the factor group

$$\mathbb{Q}^* \langle \sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r} \rangle / \mathbb{Q}^*.$$

Roughly speaking, Cogalois Theory investigates finite *radical extensions*, i.e.,

$$F(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r})/F$$

where $F$ is an arbitrary field, $r, n_1, \ldots, n_r \in \mathbb{N}^*$, $a_1, \ldots, a_r \in F^*$ and $\sqrt[n_i]{a_i} \in \Omega$ is an $n_i$-th root of $a_i$, $\forall\, i$, $1 \leqslant i \leqslant r$. In the most cases

$$\Delta = F^* \langle \sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r} \rangle / F^*.$$

In our opinion, this theory was born in 1986 when the fundamental paper of *Cornelius Greither* and *David K. Harrison* [15] has been published. Note that, like in the case of Galois Theory, where an infinite Galois Theory exists, an *infinite Cogalois Theory* has been invented in 2001 by Albu and Ţena [5]. Further, the infinite Cogalois Theory has been generalized in 2005 to arbitrary profinite groups by Albu and Basarab [2], leading to a so called *abstract Cogalois Theory* for such groups.

We are now going to present the basic concept of Cogalois Theory, namely that of *G-Cogalois extension* we referred after Remark 2.10. To do that, we need first to define the following notions: *Cogalois group, radical extension, Cogalois extension, G-radical extension, G-Kneser extension, strongly G-Kneser extension,* and *Kneser group.*

For any extension $E/F$ we denote

$$T(E/F) := \{\, x \in E^* \mid x^n \in F^* \text{ for some } n \in \mathbb{N}^* \,\}.$$

Clearly $F^* \leqslant T(E/F) \leqslant E^*$, so it makes sense to consider the quotient group $T(E/F)/F^*$, which is nothing else than the torsion group $t(E^*/F^*)$ of the

quotient group $E^*/F^*$, called the *Cogalois group* of the extension $E/F$ and denoted by $\mathrm{Cog}\,(E/F)$. This group, introduced by Greither and Harrison [15], plays a major role in Cogalois Theory and is somewhat dual to the Galois group of $E/F$, which explains the terminology.

Notice that the Cogalois group of a finite extension could be infinite, but a nice result due to Greither and Harrison [15] states that the Cogalois group of any extension of algebraic number fields is finite. Recall that an *algebraic number field* is any subfield $K$ of $\mathbb{C}$ such that $K/\mathbb{Q}$ is a finite extension.

Observe that for every element $x \in T(E/F)$ there exists an $n \in \mathbb{N}^*$ such that $x^n = a \in F$, and in this case $x$ is usually denoted by $\sqrt[n]{a}$ and is called an $n$-th *radical* of $a$. Thus, $T(E/F)$ is precisely the set of all "radicals" belonging to $E$ of elements of $F^*$. This observation suggests to define a *radical extension* as being an extension $E/F$ such that $E$ is obtained by adjoining to the base field $F$ an arbitrary set $R$ of "radicals" over $F$, i.e., $E = F(R)$ for some $R \subseteq T(E/F)$. Obviously, one can replace $R$ by the subgroup $G = F^*\langle R\rangle$ generated by $F^*$ and $R$ of the multiplicative group $E^*$ of $E$. Thus, any radical extension $E/F$ has the form $E = F(G)$, where $F^* \leqslant G \leqslant T(E/F)$. Such an extension is called *$G$-radical*. A finite extension $E/F$ is said to be *$G$-Kneser* if it is $G$-radical and $|G/F^*| = [E : F]$. The extension $E/F$ is called *Kneser* if it is $G$-Kneser for some group $G$.

The next result, due to *Martin Kneser* (1928-2004), is one of the major tools of Cogalois Theory.

**Theorem 3.3** (The Kneser Criterion [17])**.** *The following assertions are equivalent for a finite separable $G$-radical extension $E/F$.*

(1) *$E/F$ is a $G$-Kneser extension.*

(2) *For every odd prime $p$, $\zeta_p \in G \Longrightarrow \zeta_p \in F$, and $1 \pm \zeta_4 \in G \Longrightarrow \zeta_4 \in F$.*

□

A subextension of a Kneser extension is not necessarily Kneser; so, it makes

sense to consider the extensions that inherit for subextensions the property of being Kneser, which will be called *strongly Kneser*. More precisely, an extension $E/F$ is said to be *strongly $G$-Kneser* if it is a finite $G$-radical extension such that, for every intermediate field $K$ of $E/F$, the extension $K/F$ is $K^* \cap G$-Kneser. The extension $E/F$ is called *strongly Kneser* if it is strongly $G$-Kneser for some group $G$. The next result relates these extensions with those possessing a Cogalois correspondence:

**Theorem 3.4.** (Albu & Nicolae [3]). *The following assertions are equivalent for a finite $G$-radical extension $E/F$.*

(1) *$E/F$ is strongly $G$-Kneser.*

(2) *$E/F$ is $G$-Kneser with $G/F^*$-Cogalois correspondence, i.e., the canonical maps*

$$\varphi : \mathbb{I}(E/F) \longrightarrow \mathbb{L}(G/F^*),\ \varphi(K) = (K \cap G)/F^*,$$
$$\psi : \mathbb{L}(G/F^*) \longrightarrow \mathbb{I}(E/F),\ \psi(H/F^*) = F(H),$$

*are isomorphisms of lattices, i.e., bijective order-preserving maps, inverse to one another.* □

In the theory of strongly $G$-Kneser extensions the most interesting are those which additionally are separable. They are called *$G$-Cogalois extensions* and are completely and intrinsically characterized by means of the following very useful criterion.

**Theorem 3.5** (THE $n$-PURITY CRITERION, Albu & Nicolae [3])**.** *The following assertions are equivalent for a finite separable $G$-radical extension $E/F$ with $\exp(G/F^*) = n \in \mathbb{N}^*$.*

(1) *$E/F$ is $G$-Cogalois.*

(2) *$E/F$ is a $G$-Kneser extension with $G/F^*$-Cogalois correspondence.*

(3) $E/F$ *is* $n$*-pure, i.e.,* $\mu_p(E) \subseteq F$ *for all* $p$*,* $p$ *odd prime or* 4*, with* $p \mid n$*.*
□

Recall that the *exponent* $\exp(T)$ of a multiplicative group $T$ with identity element $e$ is the least number $m \in \mathbb{N}^*$ (if it exists) with the property that $t^m = e$, $\forall\, t \in T$.

**Theorem 3.6.** (Albu & Nicolae [3]) *Let* $E/F$ *be an extension which is simultaneously* $G$*-Cogalois and* $H$*-Cogalois. Then* $G = H$*.* □

In view of Theorem 3.6, the group $G$ of any $G$-Cogalois extension $E/F$ is uniquely determined, so, it makes sense to define the *Kneser group* of $E/F$ as the factor group $G/F^*$, denoted by $\mathrm{Kne}(E/F)$. Observe that $\mathrm{Kne}(E/F) \leqslant \mathrm{Cog}(E/F)$.

**Examples 3.7.** $G$-Cogalois extensions play in Cogalois Theory the same role as that of Galois extensions in Galois Theory. The $n$-Purity Criterion (Theorem 3.5) provides plenty of such extensions:

(A) $\mathbb{Q}\left(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\right)/\mathbb{Q}$, with

$$\mathrm{Kne}\left(\mathbb{Q}\left(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\right)/\mathbb{Q}\right) = \mathbb{Q}^*\left\langle \sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r} \right\rangle/\,\mathbb{Q}.$$

(B) *Cogalois extensions* (i.e., radical extensions $E/F$ such that $|\mathrm{Cog}\,(E/F)| = [\,E : F\,]$, or equivalently, $T(E/F)$-Kneser extensions), with

$$\mathrm{Kne}(E/F) = \mathrm{Cog}\,(E/F).$$

(C) *Classical Kummer extensions* $E/F$, $E = F\left(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\right)/F$, and various of its generalizations, including *generalized Kummer extensions, Kummer extensions with few roots of unity,* and *quasi-Kummer extensions* (see Albu [1] for definitions), with

$$\mathrm{Kne}(E/F) = F^*\left\langle \sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r} \right\rangle/F^*. \qquad \square$$

## 4 Some applications of Cogalois Theory

Cogalois Theory has nice applications to elementary Field Arithmetic, to Algebraic Number Theory, to binomial ideals and Gröbner bases, etc. (see [1], [8]). Many of them cannot be performed without involving the tools of Cogalois Theory.

We present below four of these applications, especially those answering the Problems 3.1 and 3.2 discussed in the previous section. Note that most of these applications hold in a more general context.

**A1.** *Effective degree computation*: For any $r, n_1, \ldots, n_r \in \mathbb{N}^*,\ a_1, \ldots, a_r \in \mathbb{Q}_+^*$, let $\sqrt[n_i]{a_i}$ denote the positive real $n_i$-th root of $a_i,\ 1 \leqslant i \leqslant r$. Then

$$[\,\mathbb{Q}\,(\sqrt[n_1]{a_1}\,, \ldots, \sqrt[n_r]{a_r}\,) : \mathbb{Q}\,] = |\,\mathbb{Q}^*\langle \sqrt[n_1]{a_1}\,, \ldots, \sqrt[n_r]{a_r}\,\rangle/\mathbb{Q}^*|.$$

This follows immediately from the Kneser Criterion (Theorem 3.3). Indeed, the extension $\mathbb{Q}\,(\sqrt[n_1]{a_1}\,, \ldots, \sqrt[n_r]{a_r}\,)/\mathbb{Q}$ is clearly $\mathbb{Q}^*\langle \sqrt[n_1]{a_1}\,, \ldots, \sqrt[n_r]{a_r}\,\rangle$-Kneser because there are no primitive $p$-th roots of unity, $p \geqslant 3$, inside the subfield $\mathbb{Q}\,(\sqrt[n_1]{a_1}\,, \ldots, \sqrt[n_r]{a_r}\,)$ of $\mathbb{R}$. □

**A2.** *Finding effectively all intermediate fields*: We are going to describe all the subfields of $E := \mathbb{Q}\,(\sqrt[4]{12}\,, \sqrt[6]{108}\,)$, that is, all the intermediate fields of the extension $E/\mathbb{Q}$. By Example 3.7 (A), the extension $E/\mathbb{Q}$ is $G$-Cogalois, so, by Theorem 3.5, $\mathbb{I}(E/\mathbb{Q})$ is easily described by $\mathbb{L}(\mathrm{Kne}(E/\mathbb{Q}))$, where $\mathrm{Kne}(E/\mathbb{Q}) = \mathbb{Q}^*\langle \widehat{\sqrt[4]{12}}\,, \widehat{\sqrt[6]{108}}\,\rangle/\,\mathbb{Q}^*$ and $\widehat{x}$ denotes for any $x \in \mathbb{R}^*$ its coset $x\mathbb{Q}^*$ in the quotient group $\mathbb{R}^*/\mathbb{Q}^*$.

A simple calculation shows that $\mathrm{Kne}(E/\mathbb{Q})$ is a cyclic group of order 12 generated by $\widehat{c}$, where $c = \sqrt[4]{12} \cdot \sqrt[6]{108} = \sqrt[12]{20,155,392}$. Consequently all its subgroups are precisely:

$$\langle \widehat{c}\,\rangle,\ \langle \widehat{c^2}\,\rangle,\ \langle \widehat{c^3}\,\rangle,\ \langle \widehat{c^4}\,\rangle,\ \langle \widehat{c^6}\,\rangle,\ \langle \widehat{c^{12}}\,\rangle.$$

Thus, all the subfields of $E$ are exactly

$$\mathbb{Q},\ \mathbb{Q}(c),\ \mathbb{Q}(c^2),\ \mathbb{Q}(c^3),\ \mathbb{Q}(c^4),\ \mathbb{Q}(c^6),$$

where $c = \sqrt[12]{20,155,392}$. □

**A3.** *Finding effectively a primitive element*: Let $F$ be an arbitrary subfield of $\mathbb{R}$, let $k, n_1, \ldots, n_k \in \mathbb{N}^*$, let $a_1, \ldots, a_k \in F_+^*$ and let $\sqrt[n_i]{a_i}$ denote the positive real $n_i$-th root of $a_i$, $1 \leqslant i \leqslant r$. Then

$$F(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}) = F(\sqrt[n_1]{a_1} + \cdots + \sqrt[n_r]{a_r}).$$

Indeed, by the $n$-Purity Criterion (Theorem 3.5), the extension $F(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r})/F$ is $G$-Cogalois because $F(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}) \subseteq \mathbb{R}$, and hence there are no primitive $p$-th roots of unity, $p \geqslant 3$, inside $F(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r})$. By Albu [1, Corollary 8.1.4], $\sqrt[n_1]{a_1} + \cdots + \sqrt[n_r]{a_r}$ is a primitive element of the extension $F(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r})/F$. □

**A4.** *The generalized Folklore Theorem*: With the notation and hypotheses of A3, one has

$$\sqrt[n_1]{a_1} + \cdots + \sqrt[n_k]{a_k} \in F \iff \sqrt[n_i]{a_i} \in F, \ \forall\ i, 1 \leqslant i \leqslant k,$$

Indeed, assume that $\sqrt[n_1]{a_1} + \cdots + \sqrt[n_k]{a_k} \in F$. Then

$$F\left(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\right) = F(\sqrt[n_1]{a_1} + \cdots + \sqrt[n_r]{a_r}) = F$$

by A3, so $\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r} \in F$, as desired. □

## Acknowledgment

The author gratefully acknowledges partial financial support from the grant PN II - IDEI 443, code 1190/2008, awarded by the CNCSIS - UEFISCSU, Romania.

## References

[1] T. Albu, "*Cogalois Theory*", A Series of Monographs and Textbooks, Vol. 252, Marcel Dekker, Inc., New York and Basel, 2003.

[2] T. Albu and Ş.A. Basarab, *An Abstract Cogalois Theory for profinite groups*, J. Pure Appl. Algebra **200** (2005), 227-250.

[3] T. Albu and F. Nicolae, *Kneser field extensions with Cogalois correspondence*, J. Number Theory **52** (1995), 299-318.

[4] T. Albu and F. Nicolae, *G-Cogalois field extensions and primitive elements*, in "Symposia Gaussiana", Conference A: Mathematics and Theoretical Physics, Eds. M. Behara, R. Fritsch, and R.G. Lintz, Walter de Gruyter & Co., Berlin New York, 1995, pp. 233-240.

[5] T. Albu and M. Ţena, *Infinite Cogalois Theory*, Math. Rep. **3 (53)** (2001), 105-132.

[6] R. Apéry, *Irrationalité de* $\zeta(2)$ *et* $\zeta(3)$, Astérisque **61** (1979), 11-13.

[7] K. Ball & T. Rivoal, *Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs*, Invent. Math. **146** (2001) 193-207.

[8] E. Becker, R. Grobe, and M. Niermann, *Radicals of binomial ideals*, J. Pure Appl. Algebra **117 & 118** (1997), 41-79.

[9] A. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. **15** (1940), 3-6.

[10] F. Beukers, *A note on the irrationality of* $\zeta(2)$ *and* $\zeta(3)$, Bull. London Math. Soc. **11** (1979), 268-272.

[11] Z.I. Borevitch and I.R. Shafarevitch, "*Number Theory*", Academic Press, New York, 1966.

[12] N. Bourbaki, "*Algèbre*", Chapitres 4 à 7, Masson, Paris, 1981.

[13] A. Froda, *Critéres paramétriques d'irrationalité*, Math. Scand. **12** (1963), 199-208.

[14] A. Froda, *La constante d'Euler est irrationelle*, Atti Accad. Naz. Lincei Rend. **38** (1965), 338-344.

[15] C. Greither and D.K. Harrison, *A Galois correspondence for radical extensions of fields*, J. Pure Appl. Algebra **43** (1986), 257-270.

[16] G. Karpilovsky, "*Topics in Field Theory*", North-Holland, Amsterdam, New York, Oxford, and Tokyo, 1989.

[17] M. Kneser, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. **26** (1975), 307-308.

[18] S. Lang, "*Algebra*", Addison-Wesley Publishing Company, Reading, Massachusetts, 1965.

[19] P. Mihăilescu, *Neue Aufgabe 835*, Elemente der Mathematik (Basel) **35** (1980), p. 22; *Lösung*, ibid. **36** (1981), pp. 19-20.

[20] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture* J. Reine Angew. Math. **572** (2004), 167-195.

[21] Yu.V. Nesterenko, *An elementary proof of the irrationality of* $\zeta(3)$ (Russian), Vestnik Moskow. Univ. Ser. I Mat. Mekh. **64** (2009), 28-35.

[22] A. van der Poorten, *A proof that Euler missed ... Apéry's proof of the irrationality of* $\zeta(3)$*. An informal report*, Math. Intelligencer **1** (1979), 195-203.

[23] T. Rivoal, *La fonction zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs*, C. R. Acad. Sci. Paris Sér. I Math. **331** (2000), 267-270.

[24] J. Sondow, *Criteria for irrationality of Euler's constant*, Proc. Amer. Math. Soc. **131** (2003), 3335-3344.

[25] www.wikipedia.org

[26] V.V. Zudilin, *One of the numbers* $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ *is irrational* (Russian), Uspekhi Mat. Nauk **56** (2001), 149-150.

"Simion Stoilow" Institute of Mathematics of the Romanian Academy
P.O. Box 1 - 764
RO - 010145 Bucharest 1, ROMANIA
e-mail: Toma.Albu@imar.ro