All Liouville Numbers are Transcendental

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Adam Naumowicz
Institute of Informatics
University of Białystok
Poland

Adam Grabowski
Institute of Informatics
University of Białystok
Poland

Summary. In this Mizar article, we complete the formalization of one of the items from Abad and Abad's challenge list of "Top 100 Theorems" about Liouville numbers and the existence of transcendental numbers. It is item #18 from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at http://www.cs.ru.nl/F.Wiedijk/100/. Liouville numbers were introduced by Joseph Liouville in 1844 [15] as an example of an object which can be approximated "quite closely" by a sequence of rational numbers. A real number x is a Liouville number iff for every positive integer n, there exist integers p and q such that $q > 1$ and

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

It is easy to show that all Liouville numbers are irrational. The definition and basic notions are contained in [10], [1], and [12]. Liouvile constant, which is defined formally in [12], is the first explicit transcendental (not algebraic) number, another notable examples are e and π [5], [11], and [4]. Algebraic numbers were formalized with the help of the Mizar system [13] very recently, by Yasushige Watase in [23] and now we expand these techniques into the area of not only pure algebraic domains (as fields, rings and formal polynomials), but also for more set-theoretic fields. Finally we show that all Liouville numbers are transcendental, based on Liouville's theorem on Diophantine approximation.

MML identifier: `LIOUVIL2`, version: `8.1.05 5.40.1286`

From now on m, n denote natural numbers, r denotes a real number, and c denotes an element of $\mathbb{C}_F$.

Let f be a non empty, complex-valued function. One can check that $|f|$ is non empty. Now we state the propositions:

(1)   If $2 \leqslant m$, then for every real number A, there exists a positive natural number n such that $A \leqslant m^n$.

(2)   Let us consider a positive real number A. Then there exists a positive natural number n such that $\frac{1}{2^n} \leqslant A$. The theorem is a consequence of (1).

Let us consider r and n. Observe that $[r - n, r + n]$ is right-ended.

Let a, b be real numbers. One can verify that $[a, b]$ is closed interval as a subset of $\mathbb{R}$ and there exists an element of $\mathbb{R}_F$ which is irrational.

(3) $\mathbb{R}_F$ is a subring of $\mathbb{C}_F$.

(4) $\mathbb{F}_{\mathbb{Q}}$ is a subring of $\mathbb{R}_F$.

(5) $\mathbb{Z}^R$ is a subring of $\mathbb{R}_F$.

Let us consider a ring R and a subring S of R. Now we state the propositions:

(6)   Every element of S is an element of R.

(7)   Every polynomial over S is a polynomial over R.

Let us consider a ring R, a subring S of R, a polynomial f over S, and a polynomial g over R. Now we state the propositions:

(8)   If $f = g$, then $\operatorname{len} f = \operatorname{len} g$.
PROOF: the length of f is at most $\operatorname{len} g$ by [20, (8)]. For every natural number m such that the length of f is at most m holds $\operatorname{len} g \leqslant m$. $\square$

(9)   If $f = g$, then $\operatorname{LC} f = \operatorname{LC} g$.

(10)   Let us consider a non degenerated ring R, a subring S of R, a polynomial f over S, and a monic polynomial g over R. If $f = g$, then f is monic. The theorem is a consequence of (8).

Let R be a non degenerated ring. Let us note that every subring of R is non degenerated and there exists a subring of R which is non degenerated.

Now we state the propositions:

(11)   Let us consider a non degenerated ring R, a non degenerated subring S of R, a monic polynomial f over S, and a polynomial g over R. If $f = g$, then g is monic. The theorem is a consequence of (8).

(12)   Let us consider a non degenerated ring R, a subring S of R, a polynomial f over S, and a non-zero polynomial g over R. If $f = g$, then f is non-zero. The theorem is a consequence of (8).

(13) Let us consider a non degenerated ring R, a subring S of R, a non-zero polynomial f over S, and a polynomial g over R. If $f = g$, then g is non-zero. The theorem is a consequence of (8).

(14) Let us consider rings R, T, a subring S of R, a polynomial f over S, and a polynomial g over R. Suppose $f = g$. Let us consider an element a of R. Then $\mathrm{ExtEval}(f, a(\in T)) = \mathrm{ExtEval}(g, a(\in T))$. The theorem is a consequence of (8).

(15) Let us consider a ring R, a subring S of R, a polynomial f over S, an element r of R, and an element s of S. If $r = s$, then $\mathrm{ExtEval}(f, r) = \mathrm{ExtEval}(f, s)$. The theorem is a consequence of (6).

(16) Let us consider a ring R, a subring S of R, an element r of R, and an element s of S. If $r = s$ and s is integral over S, then r is integral over R. The theorem is a consequence of (7), (8), (14), and (15).

(17) Let us consider a ring R, a subring S of R, an element r of R, an element s of S, a polynomial f over R, and a polynomial g over S. If $r = s$ and $f = g$ and r is a root of f, then s is a root of g.

PROOF: Consider F being a finite sequence of elements of R such that $\mathrm{eval}(f, r) = \sum F$ and $\mathrm{len}\, F = \mathrm{len}\, f$ and for every element n of $\mathbb{N}$ such that $n \in \mathrm{dom}\, F$ holds $F(n) = f(n -' 1) \cdot \mathrm{power}_R(r, n -' 1)$. For every element n of $\mathbb{N}$ such that $n \in \mathrm{dom}\, F$ holds $F(n) = g(n -' 1) \cdot \mathrm{power}_S(s, n -' 1)$ by (6), [23, (11)]. $\mathrm{rng}\, F \subseteq$ the carrier of S. Reconsider $G = F$ as a finite sequence of elements of S. $\mathrm{len}\, G = \mathrm{len}\, g$. $\sum G$ is an element of R. $\square$

(18) Every ring is a subring of R.

One can check that $\mathbf{0}.\mathbb{C}_\mathrm{F}$ is $\mathbb{Z}$-valued and $\mathbf{1}.\mathbb{C}_\mathrm{F}$ is $\mathbb{Z}$-valued.

Let L be a non degenerated, non empty double loop structure. One can check that every polynomial over L which is monic is also non-zero and there exists a polynomial over $\mathbb{C}_\mathrm{F}$ which is monic and $\mathbb{Z}$-valued and there exists a polynomial over $\mathbb{C}_\mathrm{F}$ which is monic and $\mathbb{Q}$-valued and there exists a polynomial over $\mathbb{C}_\mathrm{F}$ which is monic and $\mathbb{R}$-valued.

Now we state the propositions:

(19) Every $\mathbb{Z}$-valued polynomial over $\mathbb{C}_\mathrm{F}$ is a polynomial over $\mathbb{Z}^\mathrm{R}$.

(20) Every $\mathbb{Q}$-valued polynomial over $\mathbb{C}_\mathrm{F}$ is a polynomial over $\mathbb{F}_\mathbb{Q}$.

(21) Every $\mathbb{R}$-valued polynomial over $\mathbb{C}_\mathrm{F}$ is a polynomial over $\mathbb{R}_\mathrm{F}$.

Let L be a non empty zero structure. Let us note that every polynomial over L which is non-zero is also non zero and every polynomial over L which is zero is also non non-zero. Now we state the propositions:

(22) Let us consider an integer i, and a $\mathbb{Z}$-valued finite sequence f. If $i \in \mathrm{rng}\, f$, then $i \mid \prod f$.

PROOF: Define $\mathcal{P}$[finite sequence of elements of $\mathbb{Z}$] $\equiv$ for every integer a such that $a \in \mathrm{rng}\,\$_1$ holds $a \mid \prod \$_1$. For every finite sequence p of elements of $\mathbb{Z}$ and for every element n of $\mathbb{Z}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle n \rangle]$ by [3, (31)], [8, (96)], [14, (2)], [3, (39)]. For every finite sequence p of elements of $\mathbb{Z}$, $\mathcal{P}[p]$ from [6, Sch. 2]. $\square$

(23)   There exists a non-zero, $\mathbb{Z}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f if and only if there exists a monic, $\mathbb{Q}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f.
PROOF: If there exists a non-zero, $\mathbb{Z}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f, then there exists a monic, $\mathbb{Q}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f by [18, (5)], [16, (6)], [19, (59)]. Reconsider $l = \mathrm{len}\,f$ as an element of $\mathbb{N}$. Define $\mathcal{F}$(element of $\mathbb{N}$) $= (\mathrm{den}(f(\$_1)))(\in \mathbb{C}_{\mathrm{F}})$. Consider d being a polynomial over $\mathbb{C}_{\mathrm{F}}$ such that $\mathrm{len}\,d \leqslant l$ and for every element n of $\mathbb{N}$ such that $n < l$ holds $d(n) = \mathcal{F}(n)$ from [17, Sch. 2]. Define $\mathcal{G}$(natural number) $= d(\$_1 -' 1)$. Consider d_2 being a finite sequence such that $\mathrm{len}\,d_2 = \mathrm{len}\,d$ and for every natural number k such that $k \in \mathrm{dom}\,d_2$ holds $d_2(k) = \mathcal{G}(k)$ from [3, Sch. 2]. $\mathrm{rng}\,d_2 \subseteq \mathbb{Z}$ by [22, (25)]. Reconsider $d_3 = d_2$ as a finite sequence of elements of $\mathbb{C}_{\mathrm{F}}$. Reconsider $d_1 = \prod d_2$ as an element of $\mathbb{C}_{\mathrm{F}}$. For every natural number i such that $i \in \mathrm{dom}\,d_3$ holds $d_3(i) \neq 0_{\mathbb{C}_{\mathrm{F}}}$ by [22, (25)]. Consider d_4 being a finite sequence of elements of $\mathbb{C}$ such that $d_4 = d_2$ and $\prod d_2 = \cdot_{\mathbb{C}} \circledast d_4$. $\mathrm{rng}(d_1 \cdot f) \subseteq \mathbb{Z}$ by [20, (8)], [2, (12), (13)], [22, (25)]. $\square$

(24) c is algebraic if and only if there exists a monic, $\mathbb{Q}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f. The theorem is a consequence of (7), (8), (14), and (20).

(25) c is algebraic if and only if there exists a non-zero, $\mathbb{Z}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f. The theorem is a consequence of (24) and (23).

(26) c is algebraic integer if and only if there exists a monic, $\mathbb{Z}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f. The theorem is a consequence of (7), (8), (14), and (19).

Let us observe that every complex which is algebraic integer is also algebraic and every complex which is transcendental is also non algebraic integer.

(27)   LIOUVILLE'S THEOREM ON DIOPHANTINE APPROXIMATION:
Let us consider a non-zero, $\mathbb{Z}$-valued polynomial f over $\mathbb{R}_{\mathrm{F}}$, and an irrational element a of $\mathbb{R}_{\mathrm{F}}$. Suppose a is a root of f. Then there exists a positive real number A such that for every integer p for every positive natural number q, $|a - \frac{p}{q}| > \frac{A}{q^{\mathrm{len}\,f}}$.
PROOF: Set $n = \mathrm{len}\,f$. Set $X = [a - 1, a + 1]$. Set $E = \mathrm{Eval}(f)$. Set

$F = E ' | \restriction X$. Set $M_1 = \sup \mathrm{rng} \, |F|$. Set $M = M_1 + 1$. Consider Y being an object such that $Y \in \mathrm{rng} \, |F|$. Consider A being an object such that $A \in \mathrm{dom} \, |F|$ and $|F|(A) = Y$. Set $R_1 = \mathrm{Roots} \, f \setminus \{a\}$. Define $\mathcal{F}(\text{real number}) = |a - \$_1|$. Set $D = \{\mathcal{F}(b), \text{ where } b \text{ is an element of } \mathbb{R}_\mathrm{F} : b \in R_1\}$. D is finite from [21, Sch. 21]. $D \subseteq \mathbb{R}$. Set $M_2 = \{1, \frac{1}{M}\} \cup D$. For every real number x such that $x \in M_2$ holds $x > 0$ by [9, (56)]. Consider A being a real number such that $0 < A$ and $A < \inf M_2$. Set $q_1 = q^n$. Reconsider $q_2 = q_1$ as an element of $\mathbb{R}_\mathrm{F}$. Reconsider $p_1 = \frac{p}{q}$ as an element of $\mathbb{R}_\mathrm{F}$. Consider E_1 being a finite sequence of elements of the carrier of $\mathbb{R}_\mathrm{F}$ such that $E(\frac{p}{q}) = \sum E_1$ and $\mathrm{len} \, E_1 = \mathrm{len} \, f$ and for every element n of $\mathbb{N}$ such that $n \in \mathrm{dom} \, E_1$ holds $E_1(n) = f(n -' 1) \cdot \mathrm{power}_{\mathbb{R}_\mathrm{F}}(p_1, n -' 1)$. Set $G = q_2 \cdot E_1$. $\mathrm{rng} \, G \subseteq \mathbb{Z}$ by [3, (1)], [2, (10)], [7, (3)], [24, (50)]. $\square$

Main Result: All Liouville numbers are transcendental.

References

[1] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Springer-Verlag, 2nd edition, 1997.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Sophie Bernard, Yves Bertot, Laurence Rideau, and Pierre-Yves Strub. Formal proofs of transcendence for e and π as an application of multivariate and symmetric polynomials. In Jeremy Avigad and Adam Chlipala, editors, *Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs*, pages 76–87. ACM, 2016. doi:10.1145/2854065.2854072.

[5] Jesse Bingham. Formalizing a proof that e is transcendental. *Journal of Formalized Reasoning*, 4:71–84, 2011.

[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[8] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[10] J.H. Conway and R.K. Guy. *The Book of Numbers*. Springer-Verlag, 1996.

[11] Manuel Eberl. Liouville numbers. *Archive of Formal Proofs*, December 2015. http://isa-afp.org/entries/Liouville_Numbers.shtml, Formal proof development.

[12] Adam Grabowski and Artur Korniłowicz. Introduction to Liouville numbers. *Formalized Mathematics*, 25(**1**):39–48, 2017. doi:10.1515/forma-2017-0003.

[13] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[14] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[15] Joseph Liouville. Nouvelle démonstration d'un théorème sur les irrationnelles algébriques, inséré dans le Compte Rendu de la dernière séance. *Compte Rendu Acad. Sci. Paris*, Sér.A (18):910–911, 1844.

[16] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**):

265–269, 2001.

[17] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.

[18] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.

[19] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.

[20] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.

[21] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.

[22] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[23] Yasushige Watase. Algebraic numbers. *Formalized Mathematics*, 24(**4**):291–299, 2016. doi:10.1515/forma-2016-0025.

[24] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

Received February 23, 2017