

Basel Problem¹

Karol Pałk
Institute of Informatics
University of Białystok
Poland

Artur Kornilowicz
Institute of Informatics
University of Białystok
Poland

Summary. A rigorous elementary proof of the Basel problem [6, 1]

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

is formalized in the Mizar system [3]. This theorem is item #14 from the “Formalizing 100 Theorems” list maintained by Freek Wiedijk at <http://www.cs.ru.nl/F.Wiedijk/100/>.

MSC: 11M06 03B35

Keywords: Basel problem

MML identifier: BASEL_2, version: 8.1.06 5.43.1297

1. PRELIMINARIES

From now on k, m, n denote natural numbers, R denotes a commutative ring, p, q denote polynomials over R , and z_0, z_1 denote elements of R .

Let L be a right zeroed, non empty double loop structure. Let us consider n . Let us note that $n \cdot 0_L$ reduces to 0_L .

Now we state the proposition:

- (1) Let us consider a complex z , and an element e of \mathbb{C}_F . If $z = e$, then $n \cdot z = n \cdot e$.

Let e be an element of \mathbb{C}_F and z be a complex. Let us consider n . We identify $n \cdot z$ with $n \cdot e$. Now we state the propositions:

¹This work has been financed by the resources of the Polish National Science Centre granted by decision no. DEC-2015/19/D/ST6/01473.

- (2) Let us consider a complex-valued finite sequence Z , and a finite sequence E of elements of \mathbb{C}_F . If $E = Z$, then $\sum Z = \sum E$.

PROOF: Consider f being a sequence of \mathbb{C}_F such that $\sum E = f(\text{len } E)$ and $f(0) = 0_{\mathbb{C}_F}$ and for every natural number j and for every element v of \mathbb{C}_F such that $j < \text{len } E$ and $v = E(j+1)$ holds $f(j+1) = f(j) + v$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 \leq \text{len } Z$, then $\sum(Z|\$1) = f(\$1)$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by [2, (11)], [15, (25)], [5, (10)], [2, (13)]. $\mathcal{P}[n]$ from [2, Sch. 2]. \square

- (3) $(\mathbf{1}_{\mathbb{C}_F})^n = \mathbf{1}_{\mathbb{C}_F}$.

- (4) Let us consider a left zeroed, right zeroed, non empty additive loop structure L , and elements z_0, z_1 of L . Then $\langle z_0, z_1 \rangle = \langle z_0 \rangle + \langle 0_L, z_1 \rangle$.

- (5) Let us consider an add-associative, right zeroed, right complementable, distributive, non empty double loop structure L , and elements a, b, c, d of L . Then $\langle a, b \rangle * \langle c, d \rangle = \langle a \cdot c, a \cdot d + (b \cdot c), b \cdot d \rangle$.

- (6) Let us consider an Abelian, add-associative, right zeroed, right complementable, well unital, commutative, distributive, non empty double loop structure L . Then $\langle 0_L, 0_L, 1_L \rangle = \langle 0_L, 1_L \rangle^2$. The theorem is a consequence of (5).

- (7) Let us consider a right zeroed, add-associative, right complementable, right distributive, non empty double loop structure L , an element z of L , and a polynomial p over L . Then $(p * \langle z \rangle)(n) = p(n) \cdot z$.

PROOF: Set $Z = \langle z \rangle$. Consider r being a finite sequence of elements of the carrier of L such that $\text{len } r = n+1$ and $(p * \langle z \rangle)(n) = \sum r$ and for every element k of \mathbb{N} such that $k \in \text{dom } r$ holds $r(k) = p(k - '1) \cdot Z(n+1 - 'k)$. Set $l = \text{len } r$. For every element k of \mathbb{N} such that $k \in \text{dom } r$ and $k \neq l$ holds $r_k = 0_L$ by [15, (25)], [2, (14)], [11, (32)]. \square

- (8) Let us consider an Abelian, add-associative, right zeroed, right complementable, well unital, associative, commutative, distributive, non empty double loop structure L , and an element x of L . Then $\langle x \rangle^n = \langle x^n \rangle$.

PROOF: Set $X = \langle x \rangle$. Define $\mathcal{P}[\text{natural number}] \equiv X^{\$1} = \langle x^{\$1} \rangle$. $\mathcal{P}[0]$ by [13, (8)], [2, (14)], [11, (32)], [9, (30)]. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [11, (19)], [2, (14)], [11, (32)], [13, (8)]. For every n , $\mathcal{P}[n]$ from [2, Sch. 2]. \square

- (9) (i) $\langle z_0, z_1 \rangle^0(0) = 1_R$, and

(ii) if $n > 0$, then $\langle 0_R, z_1 \rangle^n(n) = z_1^n$, and

(iii) if $k \neq n$, then $\langle 0_R, z_1 \rangle^n(k) = 0_R$.

PROOF: Set $P = \langle 0_R, z_1 \rangle$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 > 0$, then $P^{\$1}(\$1) = z_1^{\$1}$ and for every k such that $k \neq \$1$ holds $P^{\$1}(k) = 0_R$. $\mathcal{P}[0]$ by [11, (15)], [9, (30)]. For every natural number i such that $\mathcal{P}[i]$ holds

$\mathcal{P}[i + 1]$ by [11, (19), (16), (38)], [13, (8)]. For every natural number i , $\mathcal{P}[i]$ from [2, Sch. 2]. \square

(10) (i) $\langle 0_R, 0_R, \mathbf{1}_R \rangle^n (2 \cdot n) = \mathbf{1}_R$, and

(ii) for every k such that $k \neq 2 \cdot n$ holds $\langle 0_R, 0_R, \mathbf{1}_R \rangle^n (k) = 0_R$.

PROOF: Set $x_1 = \langle 0_R, \mathbf{1}_R \rangle$. Set $x_2 = \langle 0_R, 0_R, \mathbf{1}_R \rangle$. Define $\mathcal{P}[\text{natural number}] \equiv x_2^{\$1} = x_1^{2 \cdot \$1}$. If $\mathcal{P}[k]$, then $\mathcal{P}[k + 1]$ by (6), [11, (17), (19)], [9, (33)]. $\mathcal{P}[k]$ from [2, Sch. 2]. Define $\mathcal{Q}[\text{natural number}] \equiv (\mathbf{1}_R)^{\$1} = \mathbf{1}_R$. If $\mathcal{Q}[k]$, then $\mathcal{Q}[k + 1]$. $\mathcal{Q}[k]$ from [2, Sch. 2]. \square

(11) Let us consider an integral domain L , and a non-zero polynomial p over L . Then $\overline{\text{Roots}(p)} < \text{len } p$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non-zero polynomial p over L such that $\text{len } p = \$1$ holds $\overline{\text{Roots}(p)} < \text{len } p$. For every natural number n such that $n \geq 1$ and $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$ by [12, (47)], [10, (3)], [12, (50), (23), (48)]. For every natural number n such that $n \geq 1$ holds $\mathcal{P}[n]$ from [2, Sch. 8]. \square

Let L be an add-associative, right zeroed, right complementable, distributive, non empty double loop structure and a be a polynomial over L . The functor ${}^{\textcircled{a}}$ yielding an element of $\text{PolyRing}(L)$ is defined by the term

(Def. 1) a .

Let n be a natural number. The functor $n \cdot a$ yielding a polynomial over L is defined by the term

(Def. 2) $n \cdot {}^{\textcircled{a}}$.

Now we state the propositions:

(12) Let us consider an add-associative, right zeroed, right complementable, distributive, non empty double loop structure L , and a polynomial a over L . Then $(n \cdot a)(k) = n \cdot a(k)$.

(13) $\langle z_0, z_1 \rangle^n (k) = \binom{n}{k} \cdot (z_1^k \cdot z_0^{n-k})$.

PROOF: Set $Z_0 = \langle z_0 \rangle$. Set $Z_1 = \langle 0_R, z_1 \rangle$. Set $C = \binom{n}{k} \cdot (z_1^k \cdot z_0^{n-k})$. Set $P_2 = \text{PolyRing}(R)$. $\langle z_0, z_1 \rangle = Z_0 + Z_1$. Consider F being a finite sequence of elements of $\text{PolyRing}(R)$ such that $\langle z_0, z_1 \rangle^n = \sum F$ and $\text{len } F = n + 1$ and for every natural number k such that $k \leq n$ holds $F(k + 1) = \binom{n}{k} \cdot Z_1^k * Z_0^{n-k}$. For every natural number i such that $i \leq n$ and for every polynomial F_1 over R such that $F_1 = F(i + 1)$ holds if $k \neq i$, then $F_1(k) = 0_R$ and if $k = i$, then $F_1(k) = C$ by (12), (8), (7), (9). Consider f being a sequence of the carrier of P_2 such that $\sum F = f(\text{len } F)$ and $f(0) = 0_{P_2}$ and for every natural number j and for every element v of P_2 such that $j < \text{len } F$ and $v = F(j + 1)$ holds $f(j + 1) = f(j) + v$. For every polynomial p over R such that $p = f(0)$ holds $p(k) = 0_R$ by [14, (7)]. \square

2. IMAGINARY COMPLEX NUMBERS

Let z be a complex. We say that z is imaginary if and only if

(Def. 3) $\Re(z) = 0$.

Note that i is imaginary and every complex which is real and imaginary is also zero and every complex which is zero is also imaginary.

Let z_1, z_2 be imaginary complexes. One can verify that $z_1 \cdot z_2$ is real and $z_1 + z_2$ is imaginary.

Let z be an imaginary complex and r be a real complex. Note that $z \cdot r$ is imaginary and $0_{\mathbb{C}_F}$ is real and imaginary and there exists an element of \mathbb{C}_F which is real and imaginary.

Let z be a real element of \mathbb{C}_F and n be a natural number. Observe that $n \cdot z$ is real.

Let z be an imaginary element of \mathbb{C}_F . Observe that $n \cdot z$ is imaginary.

Let z be an imaginary complex and n be an even natural number. Let us observe that $\text{power}_{\mathbb{C}_F}(z, n)$ is real.

Let n be an odd natural number. One can check that $\text{power}_{\mathbb{C}_F}(z, n)$ is imaginary as a complex.

Let r be a real element of \mathbb{C}_F and n be a natural number. Let us note that $\text{power}_{\mathbb{C}_F}(r, n)$ is real and every element of \mathbb{C}_F which is zero is also imaginary and real.

Let p be a sequence of \mathbb{C}_F . We say that p is imaginary if and only if

(Def. 4) for every natural number i , $p(i)$ is imaginary.

Let i_1 be an imaginary element of \mathbb{C}_F . One can check that $\langle i_1 \rangle$ is imaginary.

Let i_2 be an imaginary element of \mathbb{C}_F . Observe that $\langle i_1, i_2 \rangle$ is imaginary and there exists a polynomial over \mathbb{C}_F which is imaginary.

Now we state the propositions:

(14) Let us consider an imaginary polynomial I over \mathbb{C}_F , and a real element r of \mathbb{C}_F . Then $\text{eval}(I, r)$ is imaginary.

PROOF: Consider H being a finite sequence of elements of \mathbb{C}_F such that $\text{eval}(I, r) = \sum H$ and $\text{len } H = \text{len } I$ and for every element n of \mathbb{N} such that $n \in \text{dom } H$ holds $H(n) = I(n - '1) \cdot \text{power}_{\mathbb{C}_F}(r, n - '1)$. Consider h being a sequence of the carrier of \mathbb{C}_F such that $\sum H = h(\text{len } H)$ and $h(0) = 0_{\mathbb{C}_F}$ and for every natural number j and for every element v of \mathbb{C}_F such that $j < \text{len } H$ and $v = H(j + 1)$ holds $h(j + 1) = h(j) + v$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 \leq \text{len } H$, then $h(\$1)$ is imaginary. If $\mathcal{P}[n]$, then $\mathcal{P}[n + 1]$ by [2, (11)], [15, (25)], [2, (13)]. $\mathcal{P}[n]$ from [2, Sch. 2]. \square

(15) Let us consider a real polynomial R over \mathbb{C}_F , and a real element r of \mathbb{C}_F . Then $\text{eval}(R, r)$ is real.

PROOF: Consider H being a finite sequence of elements of \mathbb{C}_F such that $\text{eval}(I, r) = \sum H$ and $\text{len } H = \text{len } I$ and for every element n of \mathbb{N} such that $n \in \text{dom } H$ holds $H(n) = I(n - '1) \cdot \text{power}_{\mathbb{C}_F}(r, n - '1)$. Consider h being a sequence of the carrier of \mathbb{C}_F such that $\sum H = h(\text{len } H)$ and $h(0) = 0_{\mathbb{C}_F}$ and for every natural number j and for every element v of \mathbb{C}_F such that $j < \text{len } H$ and $v = H(j + 1)$ holds $h(j + 1) = h(j) + v$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 \leq \text{len } H$, then $h(\$1)$ is real. If $\mathcal{P}[n]$, then $\mathcal{P}[n + 1]$ by [2, (11)], [15, (25)], [2, (13)]. $\mathcal{P}[n]$ from [2, Sch. 2]. \square

Let us consider an imaginary element i_3 of \mathbb{C}_F and a real element r of \mathbb{C}_F .

- (16) If n is even, then the even part of $\langle i_3, r \rangle^n$ is real and the odd part of $\langle i_3, r \rangle^n$ is imaginary. The theorem is a consequence of (13).
- (17) If n is odd, then the even part of $\langle i_3, r \rangle^n$ is imaginary and the odd part of $\langle i_3, r \rangle^n$ is real. The theorem is a consequence of (13).
- (18) Let us consider a non empty zero structure L , and a polynomial p over L . Suppose $\text{len}(\text{the even part of } p) \neq 0$. Then $\text{len}(\text{the even part of } p)$ is odd.

PROOF: Set $E = \text{the even part of } p$. Consider n such that $2 \cdot n = \text{len } E$. Reconsider $n_1 = n - 1$ as a natural number. The length of E is at most $n + n_1$ by [2, (13)]. \square

3. MAIN FACTS

Let L be a non empty set, p be a sequence of L , and m be a natural number. The functor $\text{sieve}_m(p)$ yielding a sequence of L is defined by

(Def. 5) for every natural number i , $it(i) = p(m \cdot i)$.

Let L be a non empty zero structure, p be a finite-Support sequence of L , and m be a non zero natural number. Let us observe that $\text{sieve}_m(p)$ is finite-Support.

Now we state the propositions:

- (19) Let us consider a non empty zero structure L , and a sequence p of L . Then $\text{sieve}_{(2 \cdot k)}(p) = \text{sieve}_{(2 \cdot k)}(\text{the even part of } p)$.
- (20) Let us consider a non empty zero structure L , and a polynomial p over L . Suppose $\text{len}(\text{the even part of } p)$ is odd. Then $2 \cdot \text{len } \text{sieve}_2(p) = \text{len}(\text{the even part of } p) + 1$.

PROOF: Set $E = \text{the even part of } p$. Set $C = \text{sieve}_2(E)$. Consider n such that $\text{len } E = 2 \cdot n + 1$. Set $n_1 = n + 1$. The length of C is at most n_1 by [2, (13)]. For every natural number m such that the length of C is at most m holds $n_1 \leq m$ by [2, (13)]. $C = \text{sieve}_2(p)$. \square

- (21) Let us consider a non empty zero structure L , and a polynomial p over L . Suppose $\text{len}(\text{the even part of } p) = 0$. Let us consider a non zero natural number n . Then $\text{len sieve}_{(2 \cdot n)}(p) = 0$.
- (22) Let us consider a field L , and a polynomial p over L . Then the even part of $p = (\text{sieve}_2(p))[(0_L, 0_L, \mathbf{1}_L)]$. The theorem is a consequence of (10), (18), (20), and (21).
- (23) $(\text{sieve}_2(\langle i_{\mathbb{C}_F}, 1_{\mathbb{C}_F} \rangle^{2 \cdot n+1}))(n) = \binom{2 \cdot n+1}{1} \cdot i_{\mathbb{C}_F}$. The theorem is a consequence of (3) and (13).
- (24) Suppose $n \geq 1$. Then $(\text{sieve}_2(\langle i_{\mathbb{C}_F}, 1_{\mathbb{C}_F} \rangle^{2 \cdot n+1}))(n - 1) = \binom{2 \cdot n+1}{3} \cdot -i_{\mathbb{C}_F}$. The theorem is a consequence of (3) and (13).
- (25) $\text{len sieve}_2(\langle i_{\mathbb{C}_F}, 1_{\mathbb{C}_F} \rangle^{2 \cdot n+1}) = n + 1$.
 PROOF: Set $P_1 = \langle i_{\mathbb{C}_F}, 1_{\mathbb{C}_F} \rangle^{2 \cdot n+1}$. The length of $\text{sieve}_2(P_1)$ is at most $n + 1$. For every m such that the length of $\text{sieve}_2(P_1)$ is at most m holds $n + 1 \leq m$ by [2, (13)], (23). \square

Let n be a natural number. Let us note that $\text{sieve}_2(\langle i_{\mathbb{C}_F}, 1_{\mathbb{C}_F} \rangle^{2 \cdot n+1})$ is non-zero.

- (26) $\text{rng}(^2\text{cot x-r-seq}(n)) \subseteq \text{Roots}(\text{sieve}_2(\langle i_{\mathbb{C}_F}, 1_{\mathbb{C}_F} \rangle^{2 \cdot n+1}))$.
 PROOF: Set $f = \text{x-r-seq}(n)$. Set $f_1 = ^2\text{cot } f$. Set $P_1 = \langle i_{\mathbb{C}_F}, 1_{\mathbb{C}_F} \rangle^{2 \cdot n+1}$. Consider x being an object such that $x \in \text{dom } f_1$ and $f_1(x) = y$. Reconsider $c = \text{cot}(f(x))$ as an element of \mathbb{C}_F . Set $N = 2 \cdot n + 1$. $(\text{cot}(f(x)) + i)^N$ is real by [7, (21)], [15, (29), (25)], [7, (23)]. $\text{eval}(\text{the even part of } P_1, c) = 0$ by [8, (74)], [4, (6)], [8, (8)], (17). Set $X_2 = \langle 0_{\mathbb{C}_F}, 0_{\mathbb{C}_F}, \mathbf{1}_{\mathbb{C}_F} \rangle$. The even part of $P_1 = (\text{sieve}_2(P_1))[X_2]$. \square
- (27) $\text{Roots}(\text{sieve}_2(\langle i_{\mathbb{C}_F}, 1_{\mathbb{C}_F} \rangle^{2 \cdot n+1})) = \text{rng}(^2\text{cot x-r-seq}(n))$.
 The theorem is a consequence of (26), (11), and (25).
- (28) $\sum(^2\text{cot x-r-seq}(m)) = \frac{2 \cdot m \cdot (2 \cdot m - 1)}{6}$. The theorem is a consequence of (25), (27), (23), (24), and (2).
- (29) $\sum(^2\text{cosec x-r-seq}(m)) = \frac{2 \cdot m \cdot (2 \cdot m + 2)}{6}$. The theorem is a consequence of (28).
- (30) $(\text{Basel-seq}^1)(m) \leq \sum_{\kappa=0}^m \text{Basel-seq}(\kappa)$. The theorem is a consequence of (28).
- (31) $\sum_{\kappa=0}^m \text{Basel-seq}(\kappa) \leq (\text{Basel-seq}^2)(m)$. The theorem is a consequence of (29).
- (32) **BASEL PROBLEM:**
 $\sum \text{Basel-seq} = \frac{\pi^2}{6}$. The theorem is a consequence of (30) and (31).

Note that $(\sum_{\alpha=0}^{\kappa} (\text{Basel-seq})(\alpha))_{\kappa \in \mathbb{N}}$ is non summable as a sequence of real numbers.

REFERENCES

- [1] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK*. Springer-Verlag, Berlin Heidelberg New York, 2004.
- [2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(1):41–46, 1990.
- [3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8.17.
- [4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(3):507–513, 1990.
- [5] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(2):241–245, 1996.
- [6] Augustin Louis Cauchy. *Cours d'analyse de l'Ecole royale polytechnique*. de l'Imprimerie royale, 1821.
- [7] Artur Korniłowicz and Karol Pąk. Basel problem – preliminaries. *Formalized Mathematics*, 25(2):141–147, 2017. doi:10.1515/forma-2017-0013.
- [8] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(2):265–269, 2001.
- [9] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(2):339–346, 2001.
- [10] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(2):391–395, 2001.
- [11] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(3):461–470, 2001.
- [12] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(1):49–58, 2004.
- [13] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(3):559–564, 2001.
- [14] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(2):329–334, 1990.
- [15] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(3):569–573, 1990.

Received June 27, 2017



The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.