FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 115–125, 2013
DOI: 10.2478/forma-2013-0013

VERSITA
degruyter.com/view/j/forma

Gaussian Integers[1]

Yuichi Futa
Japan Advanced Institute
of Science and Technology
Ishikawa, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Daichi Mizushima[2]
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. Gaussian integer is one of basic algebraic integers. In this article we formalize some definitions about Gaussian integers [27]. We also formalize ring (called Gaussian integer ring), $\mathbb{Z}$-module and $\mathbb{Z}$-algebra generated by Gaussian integer mentioned above. Moreover, we formalize some definitions about Gaussian rational numbers and Gaussian rational number field. Then we prove that the Gaussian rational number field and a quotient field of the Gaussian integer ring are isomorphic.

MSC: 11R04 03B35

Keywords: formalization of Gaussian integers; algebraic integers

MML identifier: GAUSSINT, version: 8.1.02 5.17.1179

The notation and terminology used in this paper have been introduced in the following articles: [5], [1], [2], [6], [12], [11], [7], [8], [18], [24], [23], [16], [19], [21], [3], [9], [20], [14], [4], [28], [25], [22], [26], [15], [17], [10], and [13].

1. Gaussian Integer Ring

Now we state the proposition:

(1) Let us consider natural numbers x, y. If $x+y=1$, then $x=1$ and $y=0$ or $x=0$ and $y=1$. Proof: $x \leqslant 1$. □

[1]This work was supported by JSPS KAKENHI 21240001 and 22300285.

[2]This research was presented during the 2012 International Symposium on Information Theory and its Applications (ISITA2012) in Honolulu, USA.

ISSN 1426–2630(Print), 1898-9934(Online)

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

(Def. 1) $\Re(z), \Im(z) \in \mathbb{Z}$.

Note that every integer is Gaussian integer.

An element of Gaussian integers is a Gaussian integer complex. Let z be an element of Gaussian integers. Note that $\Re(z)$ is integer and $\Im(z)$ is integer.

Let z_1, z_2 be elements of Gaussian integers. One can verify that $z_1 + z_2$ is Gaussian integer and $z_1 - z_2$ is Gaussian integer and $z_1 \cdot z_2$ is Gaussian integer and i is Gaussian integer.

Let z be an element of Gaussian integers. Let us note that $-z$ is Gaussian integer and $\overline{z}$ is Gaussian integer.

Let n be an integer. One can check that $n \cdot z$ is Gaussian integer.

The set of Gaussian integers yielding a subset of $\mathbb{C}$ is defined by the term

(Def. 2) the set of all z where z is an element of Gaussian integers.

Note that the set of Gaussian integers is non empty.

Let i be an integer. Let us observe that $i(\in$ the set of Gaussian integers) reduces to i.

Let us consider a set x. Now we state the propositions:

(2) If $x \in$ the set of Gaussian integers, then x is an element of Gaussian integers.

(3) If x is an element of Gaussian integers, then $x \in$ the set of Gaussian integers.

The addition of Gaussian integers yielding a binary operation on the set of Gaussian integers is defined by the term

(Def. 3) $+_{\mathbb{C}} \restriction$ the set of Gaussian integers.

The multiplication of Gaussian integers yielding a binary operation on the set of Gaussian integers is defined by the term

(Def. 4) $\cdot_{\mathbb{C}} \restriction$ the set of Gaussian integers.

The scalar multiplication of Gaussian integers yielding a function from $\mathbb{Z} \times$ the set of Gaussian integers into the set of Gaussian integers is defined by the term

(Def. 5) $\cdot_{\mathbb{C}} \restriction (\mathbb{Z} \times$ the set of Gaussian integers).

Now we state the propositions:

(4) Let us consider elements z, w of Gaussian integers. Then (the addition of Gaussian integers)$(z, w) = z + w$.

(5) Let us consider an element z of Gaussian integers and an integer i. Then (the scalar multiplication of Gaussian integers)$(i, z) = i \cdot z$.

The Gaussian integer module yielding a strict non empty $\mathbb{Z}$-module structure is defined by the term

(Def. 6) ⟨the set of Gaussian integers, 0(∈ the set of Gaussian integers), the addition of Gaussian integers, the scalar multiplication of Gaussian integers⟩.

Observe that the Gaussian integer module is Abelian add-associative right zeroed right complementable scalar distributive vector distributive scalar associative and scalar unital.

Now we state the proposition:

(6) Let us consider elements z, w of Gaussian integers. Then (the multiplication of Gaussian integers)$(z, w) = z \cdot w$.

The Gaussian integer ring yielding a strict non empty double loop structure is defined by the term

(Def. 7) ⟨the set of Gaussian integers, the addition of Gaussian integers, the multiplication of Gaussian integers, 1(∈ the set of Gaussian integers), 0(∈ the set of Gaussian integers)⟩.

One can check that the Gaussian integer ring is Abelian add-associative right zeroed right complementable associative well unital and distributive, and the Gaussian integer ring is integral domain-like, and the Gaussian integer ring is commutative.

Now we state the propositions:

(7) Every element of the Gaussian integer ring is an element of Gaussian integers.

(8) Every element of Gaussian integers is an element of the Gaussian integer ring.

2. $\mathbb{Z}$-Algebra

We consider $\mathbb{Z}$-algebra structures which extend double loop structures and $\mathbb{Z}$-module structures and are systems

⟨a carrier, a multiplication, an addition, an external multiplication,

a one, a zero⟩

where the carrier is a set, the multiplication and the addition are binary operations on the carrier, the external multiplication is a function from $\mathbb{Z} \times$ the carrier into the carrier, the one and the zero are elements of the carrier.

Let us observe that there exists a $\mathbb{Z}$-algebra structure which is non empty.

Let I_1 be a non empty $\mathbb{Z}$-algebra structure. We say that I_1 is vector associative if and only if

(Def. 8) Let us consider elements x, y of I_1 and an integer a_1. Then $a_1 \cdot (x \cdot y) = (a_1 \cdot x) \cdot y$.

Let us observe that ⟨the set of Gaussian integers, (the multiplication of Gaussian integers), (the addition of Gaussian integers), (the scalar multiplication of Gaussian integers), 1(∈ the set of Gaussian integers), 0(∈ the set of Gaussian integers)⟩ is non empty and ⟨the set of Gaussian integers, (the multiplication of Gaussian integers), (the addition of Gaussian integers), (the scalar multiplication of Gaussian integers), 1(∈ the set of Gaussian integers), 0(∈ the set of Gaussian integers)⟩ is strict Abelian add-associative right zeroed right complementable commutative associative right unital right distributive vector associative scalar associative vector distributive and scalar distributive and there exists a non empty $\mathbb{Z}$-algebra structure which is strict, Abelian, add-associative, right zeroed, right complementable, commutative, associative, right unital, right distributive, vector associative, scalar associative, vector distributive, and scalar distributive.

A $\mathbb{Z}$-algebra is an Abelian add-associative right zeroed right complementable commutative associative right unital right distributive vector associative scalar associative vector distributive scalar distributive non empty $\mathbb{Z}$-algebra structure. Now we state the proposition:

(9) ⟨the set of Gaussian integers, (the multiplication of Gaussian integers), (the addition of Gaussian integers), (the scalar multiplication of Gaussian integers), 1(∈ the set of Gaussian integers), 0(∈ the set of Gaussian integers)⟩ is a right complementable associative commutative right distributive right unital Abelian add-associative right zeroed vector distributive scalar distributive scalar associative strict vector associative non empty $\mathbb{Z}$-algebra structure.

One can verify that $\mathbb{Z}$ is denumerable and the set of Gaussian integers is denumerable and the Gaussian integer ring is non degenerated.

3. Quotient Field of Gaussian Integer Ring

The Gaussian number field yielding a strict non empty double loop structure is defined by the term

(Def. 9) The field of quotients of the Gaussian integer ring.

Observe that the Gaussian number field is non degenerated almost left invertible strict Abelian associative and distributive.

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

(Def. 10) $\Re(z), \Im(z) \in \mathbb{Q}$.

One can verify that every rational number is Gaussian rational.

An element of Gaussian rationals is a Gaussian rational complex. Let z be an element of Gaussian rationals. One can verify that $\Re(z)$ is rational and $\Im(z)$ is rational.

Let z_1, z_2 be elements of Gaussian rationals. Observe that $z_1 + z_2$ is Gaussian rational and $z_1 - z_2$ is Gaussian rational and $z_1 \cdot z_2$ is Gaussian rational.

Let z be an element of Gaussian rationals and n be a rational number. One can check that $n \cdot z$ is Gaussian rational.

Let us observe that $-z$ is Gaussian rational and z^{-1} is Gaussian rational.

The set of Gaussian rationals yielding a subset of $\mathbb{C}$ is defined by the term

(Def. 11) the set of all z where z is an element of Gaussian rationals.

Let us observe that the set of Gaussian rationals is non empty and every element of Gaussian integers is Gaussian rational.

Let us consider a set x. Now we state the propositions:

(10) If $x \in$ the set of Gaussian rationals, then x is an element of Gaussian rationals.

(11) If x is an element of Gaussian rationals, then $x \in$ the set of Gaussian rationals.

Now we state the proposition:

(12) Let us consider an element p of Gaussian rationals. Then there exist elements x, y of Gaussian integers such that

(i) $y \neq 0$, and

(ii) $p = \frac{x}{y}$.

The addition of Gaussian rationals yielding a binary operation on the set of Gaussian rationals is defined by the term

(Def. 12) $+_{\mathbb{C}} \restriction$ the set of Gaussian rationals.

The multiplication of Gaussian rationals yielding a binary operation on the set of Gaussian rationals is defined by the term

(Def. 13) $\cdot_{\mathbb{C}} \restriction$ the set of Gaussian rationals.

4. RATIONAL FIELD

Let i be an integer. One can check that $i(\in \mathbb{Q})$ reduces to i.

The rational number field yielding a strict non empty double loop structure is defined by the term

(Def. 14) $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, 1(\in \mathbb{Q}), 0(\in \mathbb{Q}) \rangle$.

Now we state the propositions:

(13) (i) the carrier of the rational number field is a subset of the carrier of $\mathbb{R}_{\mathrm{F}}$, and

(ii) the addition of the rational number field = (the addition of $\mathbb{R}_{\mathrm{F}}$) $\restriction$ (the carrier of the rational number field), and

(iii) the multiplication of the rational number field = (the multiplication of $\mathbb{R}_{\mathrm{F}}$) $\restriction$ (the carrier of the rational number field), and

(iv) $1_{\alpha} = 1_{\mathbb{R}_{\mathrm{F}}}$, and

(v) $0_\alpha = 0_{\mathbb{R}_\mathrm{F}}$, and

(vi) the rational number field is right complementable, commutative, almost left invertible, and non degenerated,

where α is the rational number field. PROOF: Every element of the rational number field is right complementable. For every element v of the rational number field such that $v \neq 0_\alpha$ holds v is left invertible, where α is the rational number field. □

(14) The rational number field is a subfield of $\mathbb{R}_\mathrm{F}$.

Let us note that the rational number field is add-associative right zeroed right complementable Abelian commutative associative left and right unital distributive almost left invertible and non degenerated and the rational number field is well unital and every element of the rational number field is rational.

Let x be an element of the rational number field and y be a rational number. We identify $-y$ with $-x$ where $x = y$. Now we state the propositions:

(15) Let us consider an element x of the rational number field and a rational number x_1. If $x \neq 0_\alpha$ and $x_1 = x$, then ${x_1}^{-1} = {x_1}^{-1}$, where α is the rational number field.

(16) Let us consider elements x, y of the rational number field and rational numbers x_1, y_1. Suppose

(i) $x_1 = x$, and

(ii) $y_1 = y$, and

(iii) $y \neq 0_\alpha$.

Then $\frac{x}{y} = \frac{x_1}{y_1}$, where α is the rational number field. The theorem is a consequence of (15).

Let us consider a field K, a subfield K_1 of K, elements x, y of K, and elements x_1, y_1 of K_1. Now we state the propositions:

(17) If $x = x_1$ and $y = y_1$, then $x + y = x_1 + y_1$.

(18) If $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

Now we state the proposition:

(19) Let us consider a field K, a subfield K_1 of K, an element x of K, and an element x_1 of K_1. If $x = x_1$, then $-x = -x_1$. The theorem is a consequence of (17).

Let us consider a field K, a subfield K_1 of K, elements x, y of K, and elements x_1, y_1 of K_1. Now we state the propositions:

(20) If $x = x_1$ and $y = y_1$, then $x - y = x_1 - y_1$.

(21) If $x = x_1$ and $x \neq 0_K$, then $x^{-1} = {x_1}^{-1}$.

(22) If $x = x_1$ and $y = y_1$ and $y \neq 0_K$, then $\frac{x}{y} = \frac{x_1}{y_1}$.

Let us consider a subfield K_1 of the rational number field. Now we state the propositions:

(23) $\mathbb{N} \subseteq$ the carrier of K_1.

(24) $\mathbb{Z} \subseteq$ the carrier of K_1.

(25) The carrier of $K_1 =$ the carrier of the rational number field.

Now we state the proposition:

(26) Let us consider a strict subfield K_1 of the rational number field. Then $K_1 =$ the rational number field. The theorem is a consequence of (25).

One can verify that the rational number field is prime.

5. GAUSSIAN RATIONAL NUMBER FIELD

Let i be a rational number. Note that $i(\in$ the set of Gaussian rationals) reduces to i.

The scalar multiplication of Gaussian rationals yielding a function from (the carrier of the rational number field) $\times$ the set of Gaussian rationals into the set of Gaussian rationals is defined by the term

(Def. 15) $\cdot_{\mathbb{C}} \restriction$((the carrier of the rational number field)$\times$the set of Gaussian rationals).

Now we state the propositions:

(27) Let us consider elements z, w of Gaussian rationals. Then (the addition of Gaussian rationals)$(z, w) = z + w$.

(28) Let us consider an element z of Gaussian rationals and an element i of $\mathbb{Q}$. Then (the scalar multiplication of Gaussian rationals)$(i, z) = i \cdot z$.

The Gaussian rational module yielding a strict non empty vector space structure over the rational number field is defined by the term

(Def. 16) $\langle$the set of Gaussian rationals, the addition of Gaussian rationals, $0(\in$ the set of Gaussian rationals), the scalar multiplication of Gaussian rationals$\rangle$.

Observe that the Gaussian rational module is scalar distributive vector distributive scalar associative scalar unital add-associative right zeroed right complementable and Abelian.

Now we state the proposition:

(29) Let us consider elements z, w of Gaussian rationals. Then (the multiplication of Gaussian rationals)$(z, w) = z \cdot w$.

The Gaussian rational ring yielding a strict non empty double loop structure is defined by the term

(Def. 17) $\langle$the set of Gaussian rationals, the addition of Gaussian rationals, the multiplication of Gaussian rationals, $1(\in$ the set of Gaussian rationals), $0(\in$ the set of Gaussian rationals)$\rangle$.

Let us note that the Gaussian rational ring is add-associative right zeroed right complementable Abelian commutative associative well unital distributive almost left invertible and non degenerated.

Now we state the proposition:

(30) There exists a function I from the Gaussian number field into the Gaussian rational ring such that

(i) for every element z such that $z \in$ the carrier of the Gaussian number field there exist elements x, y of Gaussian integers and there exists an element u of Q(the Gaussian integer ring) such that $y \neq 0$ and $u = \langle x, y \rangle$ and $z = \mathrm{QClass}(u)$ and $I(z) = \frac{x}{y}$, and

(ii) I is one-to-one and onto, and

(iii) for every elements x, y of the Gaussian number field, $I(x + y) = I(x) + I(y)$ and $I(x \cdot y) = I(x) \cdot I(y)$, and

(iv) $I(0_\alpha) = 0$, and

(v) $I(1_\alpha) = 1$,

where α is the Gaussian number field. The theorem is a consequence of (2), (10), (12), (3), (6), (4), (27), and (29). Proof: Define $\mathcal{P}[\text{element}, \text{element}] \equiv$ there exist elements x, y of Gaussian integers and there exists an element u of Q(the Gaussian integer ring) such that $y \neq 0$ and $u = \langle x, y \rangle$ and $\$_1 = \mathrm{QClass}(u)$ and $\$_2 = \frac{x}{y}$. For every element z such that $z \in$ the carrier of the Gaussian number field there exists an element w such that $w \in$ the carrier of the Gaussian rational ring and $\mathcal{P}[z, w]$. Consider I being a function from the Gaussian number field into the Gaussian rational ring such that for every element z such that $z \in$ the carrier of the Gaussian number field holds $\mathcal{P}[z, I(z)]$ from [8, Sch. 1]. For every elements z_1, z_2 of the Gaussian number field, $I(z_1 + z_2) = I(z_1) + I(z_2)$ and $I(z_1 \cdot z_2) = I(z_1) \cdot I(z_2)$ by [20, (9), (5), (10)]. □

6. Gaussian Integer Ring is Euclidean

Let a_1, b_1 be elements of Gaussian integers. We say that a_1 divides b_1 if and only if

(Def. 18) There exists an element c of Gaussian integers such that $b_1 = a_1 \cdot c$.

Note that the predicate is reflexive.

Let us consider elements a_1, b_1 of the Gaussian integer ring and elements a_2, b_2 of Gaussian integers. Now we state the propositions:

(31) If $a_1 = a_2$ and $b_1 = b_2$, then if $a_1 \mid b_1$, then a_2 divides b_2.

(32) If $a_1 = a_2$ and $b_1 = b_2$, then if a_2 divides b_2, then $a_1 \mid b_1$.

Let z be an element of Gaussian rationals. Observe that the functor $\overline{z}$ yields an element of Gaussian rationals. The functor Norm z yielding a rational number is defined by the term

(Def. 19) $z \cdot \overline{z}$.

Let us observe that Norm z is non negative.

Let z be an element of Gaussian integers. Observe that Norm z is natural.

Now we state the propositions:

(33) Let us consider an element x of Gaussian rationals. Then $\operatorname{Norm} \overline{x} = \operatorname{Norm} x$.

(34) Let us consider elements x, y of Gaussian rationals. Then $\operatorname{Norm}(x \cdot y) = \operatorname{Norm} x \cdot \operatorname{Norm} y$.

Let us consider an element x of Gaussian integers. Now we state the propositions:

(35) $\operatorname{Norm} x = 1$ if and only if $x = 1$ or $x = -1$ or $x = i$ or $x = -i$.

(36) If $\operatorname{Norm} x = 0$, then $x = 0$.

Let z be an element of Gaussian integers. We say that z is unit of Gaussian integers if and only if

(Def. 20) $\operatorname{Norm} z = 1$.

Let x, y be elements of Gaussian integers. We say that x is associated to y if and only if

(Def. 21) (i) x divides y, and

(ii) y divides x.

Let us observe that the predicate is symmetric.

Let us consider elements a_1, b_1 of the Gaussian integer ring and elements a_2, b_2 of Gaussian integers. Now we state the propositions:

(37) If $a_1 = a_2$ and $b_1 = b_2$, then if a_1 is associated to b_1, then a_2 is associated to b_2.

(38) If $a_1 = a_2$ and $b_1 = b_2$, then if a_2 is associated to b_2, then a_1 is associated to b_1.

Now we state the propositions:

(39) Let us consider an element z of the Gaussian integer ring and an element z_3 of Gaussian integers. If $z_3 = z$, then z is unital iff z_3 is unit of Gaussian integers. The theorem is a consequence of (2), (6), (34), (35), and (3). PROOF: There exists an element w of the Gaussian integer ring such that $1_\alpha = z \cdot w$, where α is the Gaussian integer ring. □

(40) Let us consider elements x, y of Gaussian integers. Then x is associated to y if and only if there exists an element c of Gaussian integers such that c is unit of Gaussian integers and $x = c \cdot y$. The theorem is a consequence of (3), (38), (2), (39), (6), and (37).

(41) Let us consider an element x of Gaussian integers. Suppose

(i) $\Re(x) \neq 0$, and

(ii) $\Im(x) \neq 0$, and

(iii) $\Re(x) \neq \Im(x)$, and

(iv) $-\Re(x) \neq \Im(x)$.

Then $\overline{x}$ is not associated to x. The theorem is a consequence of (40) and (35).

(42) Let us consider elements x, y, z of Gaussian integers. Suppose

(i) x is associated to y, and

(ii) y is associated to z.

Then x is associated to z. The theorem is a consequence of (40) and (34).

Let us consider elements x, y of Gaussian integers. Now we state the propositions:

(43) If x is associated to y, then $\overline{x}$ is associated to $\overline{y}$.

(44) Suppose $\Re(y) \neq 0$ and $\Im(y) \neq 0$ and $\Re(y) \neq \Im(y)$ and $-\Re(y) \neq \Im(y)$ and $\overline{x}$ is associated to y. Then

(i) does not x divide y, and

(ii) does not y divide x.

Let p be an element of Gaussian integers. We say that p is Gaussian prime if and only if

(Def. 22) (i) $\operatorname{Norm} p > 1$, and

(ii) for every element z of Gaussian integers, does not z divide p or z is unit of Gaussian integers or z is associated to p.

Let us consider an element q of Gaussian integers. Now we state the propositions:

(45) If $\operatorname{Norm} q$ is a prime number and $\operatorname{Norm} q \neq 2$, then $\Re(q) \neq 0$ and $\Im(q) \neq 0$ and $\Re(q) \neq \Im(q)$ and $-\Re(q) \neq \Im(q)$.

(46) If $\operatorname{Norm} q$ is a prime number, then q is Gaussian prime.

Now we state the propositions:

(47) Let us consider an element q of Gaussian rationals. Then $\operatorname{Norm} q = |\Re(q)|^{\mathbf{2}} + |\Im(q)|^{\mathbf{2}}$.

(48) Let us consider an element q of $\mathbb{R}$. Then there exists an element m of $\mathbb{Z}$ such that $|q - m| \leqslant \frac{1}{2}$.

One can check that the Gaussian integer ring is Euclidean.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[5] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[6] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

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

[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

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

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Set of points on elliptic curve in projective coordinates. *Formalized Mathematics*, 19(**3**):131–138, 2011. doi:10.2478/v10037-011-0021-6.

[13] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.

[14] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[15] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

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

[17] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.

[18] Christoph Schwarzweller. The correctness of the generic algorithms of Brown and Henrici concerning addition and multiplication in fraction fields. *Formalized Mathematics*, 6(**3**): 381–388, 1997.

[19] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.

[20] Christoph Schwarzweller. The field of quotients over an integral domain. *Formalized Mathematics*, 7(**1**):69–79, 1998.

[21] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[22] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[23] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[24] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[25] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[26] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[27] André Weil. *Number Theory for Beginners*. Springer-Verlag, 1979.

[28] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received May 19, 2013