FORMALIZED MATHEMATICS
Vol. 22, No. 4, Pages 291–301, 2014
DOI: 10.2478/forma-2014-0029

DE GRUYTER OPEN
degruyter.com/view/j/forma

The First Isomorphism Theorem and Other Properties of Rings

Artur Korniłowicz
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Christoph Schwarzweller
Institute of Computer Science
University of Gdańsk
Wita Stwosza 57, 80-952 Gdańsk
Poland

Summary. Different properties of rings and fields are discussed [12], [41] and [17]. We introduce ring homomorphisms, their kernels and images, and prove the First Isomorphism Theorem, namely that for a homomorphism $f : R \longrightarrow S$ we have $R/_{\ker(f)} \cong \mathrm{Im}(f)$. Then we define prime and irreducible elements and show that every principal ideal domain is factorial. Finally we show that polynomial rings over fields are Euclidean and hence also factorial.

MSC: 13A05 13A15 03B35

Keywords: commutative algebra; ring theory; first isomorphism theorem

MML identifier: `RING_2`, version: `8.1.03 5.26.1224`

The notation and terminology used in this paper have been introduced in the following articles: [22], [31], [2], [32], [24], [5], [11], [33], [7], [8], [26], [36], [37], [39], [30], [1], [35], [27], [34], [19], [3], [4], [9], [25], [18], [28], [29], [13], [6], [42], [43], [20], [14], [38], [23], [40], [15], [16], [21], and [10].

1. Preliminaries

Let R be a non empty set, f be a non empty finite sequence of elements of R, and x be an element of dom f. Note that the functor $f(x)$ yields an element of R. Let X be a set and F_1, F_2 be X-valued finite sequences. One can verify that $F_1 \frown F_2$ is X-valued.

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

Now we state the propositions:

(1) Let us consider an add-associative, right zeroed, right complementable, distributive, well unital, non empty double loop structure R, and a finite sequence F of elements of R. Suppose there exists a natural number i such that $i \in \operatorname{dom} F$ and $F(i) = 0_R$. Then $\prod F = 0_R$.

(2) Let us consider an add-associative, right zeroed, right complementable, well unital, distributive, integral domain-like, non degenerated double loop structure R, and a finite sequence F of elements of R. Then $\prod F = 0_R$ if and only if there exists a natural number i such that $i \in \operatorname{dom} F$ and $F(i) = 0_R$. The theorem is a consequence of (1).

Let X be a set.

A chain of X is a sequence of X. Let X be a non empty set and C be a chain of X. We say that C is ascending if and only if

(Def. 1) for every natural number i, $C(i) \subseteq C(i+1)$.

We say that C is stagnating if and only if

(Def. 2) there exists a natural number i such that for every natural number j such that $j \geqslant i$ holds $C(j) = C(i)$.

Let x be an element of X. One can check that $\mathbb{N} \longmapsto x$ is ascending and stagnating as a chain of X and there exists a chain of X which is ascending and stagnating.

Now we state the proposition:

(3) Let us consider a non empty set X, an ascending chain C of X, and natural numbers i, j. If $i \leqslant j$, then $C(i) \subseteq C(j)$.

Let R be a ring. The functor Ideals R yielding a family of subsets of the carrier of R is defined by the term

(Def. 3) the set of all I where I is an ideal of R.

One can verify that Ideals R is non empty.

Now we state the propositions:

(4) Let us consider a commutative ring R, an ideal I of R, and an element a of R. If $a \in I$, then $\{a\}$–ideal $\subseteq I$.

(5) Let us consider a ring R, and an ascending chain C of Ideals R. Then $\bigcup$ the set of all $C(i)$ where i is a natural number is an ideal of R.

Let R be a non empty double loop structure and S be a right zeroed, non empty double loop structure. Let us note that $R \longmapsto 0_S$ is additive.

Let S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure. Observe that $R \longmapsto 0_S$ is multiplicative.

Let R be a well unital, non empty double loop structure and S be a well unital, non degenerated double loop structure. Note that $R \longmapsto 0_S$ is non unity-preserving.

Let R be a non empty double loop structure. One can verify that id_R is additive, multiplicative, and unity-preserving and id_R is monomorphic and epimorphic.

Let S be a right zeroed, non empty double loop structure. Observe that there exists a function from R into S which is additive.

Let S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure. Let us observe that there exists a function from R into S which is multiplicative.

Let R, S be well unital, non empty double loop structures. One can verify that there exists a function from R into S which is unity-preserving.

Let R be a non empty double loop structure and S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure. One can verify that there exists a function from R into S which is additive and multiplicative.

2. Homomorphisms, Kernel and Image

Let R, S be rings. We say that S is R-homomorphic if and only if

(Def. 4) there exists a function f from R into S such that f inherits ring homomorphism.

Let R be a ring. One can verify that there exists a ring which is R-homomorphic.

Let R be a commutative ring. Let us observe that there exists a commutative ring which is R-homomorphic and there exists a ring which is R-homomorphic.

Let R be a field. Observe that there exists a field which is R-homomorphic and there exists a commutative ring which is R-homomorphic and there exists a ring which is R-homomorphic.

Let R be a ring and S be an R-homomorphic ring. Note that there exists a function from R into S which is additive, multiplicative, and unity-preserving.

A homomorphism from R to S is an additive, multiplicative, unity-preserving function from R into S. Let R, S, T be rings, f be a unity-preserving function from R into S, and g be a unity-preserving function from S into T. Observe that $g \cdot f$ is unity-preserving as a function from R into T.

Let R be a ring and S be an R-homomorphic ring. Note that every S-homomorphic ring is R-homomorphic.

Let R, S be non empty double loop structures. We introduce R and S are isomorphic as a synonym of R is ring isomorphic to S.

Now we state the propositions:

(6) Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure R, an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure S, and an additive function f from R into S. Then $f(0_R) = 0_S$.

(7) Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure R, an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure S, an additive function f from R into S, and an element x of R. Then $f(-x) = -f(x)$. The theorem is a consequence of (6).

(8) Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure R, an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure S, an additive function f from R into S, and elements x, y of R. Then $f(x - y) = f(x) - f(y)$. The theorem is a consequence of (7).

(9) Let us consider a right unital, non empty double loop structure R, an add-associative, right zeroed, right complementable, right unital, Abelian, right distributive, integral domain-like, non empty double loop structure S, and a multiplicative function f from R into S. Then

(i) $f(1_R) = 0_S$, or

(ii) $f(1_R) = 1_S$.

Let us consider fields E, F and an additive, multiplicative function f from E into F. Now we state the propositions:

(10) $f(1_E) = 0_F$ if and only if $f = E \longmapsto 0_F$.

(11) $f(1_E) = 1_F$ if and only if f is monomorphic.

Let E, F be fields. One can check that every function from E into F which is additive, multiplicative, and unity-preserving is also monomorphic.

Let R be a ring and I be an ideal of R. The canonical homomorphism of I into quotient field yielding a function from R into $R/_I$ is defined by

(Def. 5) for every element a of R, $it(a) = [a]_{\mathrm{EqRel}(R,I)}$.

Let us note that the canonical homomorphism of I into quotient field is additive, multiplicative, and unity-preserving and the canonical homomorphism of I into quotient field is epimorphic and $R/_I$ is R-homomorphic.

Let R be an add-associative, right zeroed, right complementable, non empty double loop structure, S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure, and f be an additive function from R into S. One can check that $\ker f$ is non empty.

Let R be a non empty double loop structure and S be an add-associative, right zeroed, right complementable, non empty double loop structure. One can check that $\ker f$ is closed under addition.

Let S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure and f be a multiplicative function from R into S. Observe that $\ker f$ is left ideal.

Let S be an add-associative, right zeroed, right complementable, distributive, non empty double loop structure. Let us observe that $\ker f$ is right ideal.

Let R be a well unital, non empty double loop structure, S be a well unital, non degenerated double loop structure, and f be a unity-preserving function from R into S. Observe that $\ker f$ is proper.

Now we state the propositions:

(12) Let us consider a ring R, an R-homomorphic ring S, and a homomorphism f from R to S. Then f is monomorphic if and only if $\ker f = \{0_R\}$. The theorem is a consequence of (6) and (8).

(13) Let us consider a ring R, and an ideal I of R. Then $\ker$ the canonical homomorphism of I into quotient field $= I$.

(14) Let us consider a ring R, and a subset I of R. Then I is an ideal of R if and only if there exists an R-homomorphic ring S and there exists a homomorphism f from R to S such that $\ker f = I$. The theorem is a consequence of (13).

Let R be a ring, S be an R-homomorphic ring, and f be a homomorphism from R to S. The functor $\operatorname{Im} f$ yielding a strict double loop structure is defined by

(Def. 6) the carrier of $it = \operatorname{rng} f$ and the addition of $it =$ (the addition of S) $\restriction \operatorname{rng} f$ and the multiplication of $it =$ (the multiplication of S) $\restriction \operatorname{rng} f$ and the one of $it = 1_S$ and the zero of $it = 0_S$.

Note that $\operatorname{Im} f$ is non empty and $\operatorname{Im} f$ is Abelian, add-associative, right zeroed, and right complementable and $\operatorname{Im} f$ is associative, well unital, and distributive.

Let R be a commutative ring and S be an R-homomorphic commutative ring. One can verify that $\operatorname{Im} f$ is commutative.

Let R be a ring and S be an R-homomorphic ring. Let us note that the functor $\operatorname{Im} f$ yields a strict subring of S. The canonical homomorphism of f into quotient field yielding a function from $R/_{\ker f}$ into $\operatorname{Im} f$ is defined by

(Def. 7) for every element a of R, $it([a]_{\mathrm{EqRel}(R, \ker f)}) = f(a)$.

One can check that the canonical homomorphism of f into quotient field is additive, multiplicative, and unity-preserving and the canonical homomorphism of f into quotient field is monomorphic and epimorphic.

Let us consider a ring R, an R-homomorphic ring S, and a homomorphism f from R to S. Now we state the propositions:

(15) $R/_{\ker f}$ and $\operatorname{Im} f$ are isomorphic.

(16) If f is onto, then $R/_{\ker f}$ and S are isomorphic.

Now we state the proposition:

(17) Let us consider a ring R. Then $R/_{\{0_R\}}$ and R are isomorphic. The theorem is a consequence of (12).

Let R be a ring. Let us note that $R/_{\Omega_R}$ is trivial.

3. Units and Non Units

Let L be a right unital, non empty multiplicative loop structure. Let us note that there exists an element of L which is unital.

A unit of L is a unital element of L. Let L be an add-associative, right zeroed, right complementable, left distributive, non degenerated double loop structure. One can check that there exists an element of L which is non unital.

A non-unit of L is a non unital element of L. Note that 0_L is non unital.

Let L be a right unital, non empty multiplicative loop structure. Let us note that 1_L is unital.

Let L be an add-associative, right zeroed, right complementable, left distributive, right unital, non degenerated double loop structure. One can verify that every unit of L is non zero.

Let F be a field. Note that every non zero element of F is unital.

Let R be an integral domain and u, v be unital elements of R. One can check that $u \cdot v$ is unital.

Let us consider a commutative ring R and elements a, b of R. Now we state the propositions:

(18) $a \mid b$ if and only if $b \in \{a\}$–ideal.

(19) $a \mid b$ if and only if $\{b\}$–ideal $\subseteq \{a\}$–ideal. The theorem is a consequence of (18).

Now we state the propositions:

(20) Let us consider a commutative ring R, and an element a of R. Then a is a unit of R if and only if $\{a\}$–ideal $= \Omega_R$. The theorem is a consequence of (18).

(21) Let us consider a commutative ring R, and elements a, b of R. Then a is associated to b if and only if $\{a\}$–ideal $= \{b\}$–ideal.

4. Prime and Irreducible Elements

Let R be a right unital, non empty double loop structure and x be an element of R. We say that x is prime if and only if

(Def. 8) $x \neq 0_R$ and x is not a unit of R and for every elements a, b of R such that $x \mid a \cdot b$ holds $x \mid a$ or $x \mid b$.

We say that x is irreducible if and only if

(Def. 9) $x \neq 0_R$ and x is not a unit of R and for every element a of R such that $a \mid x$ holds a is unit of R or associated to x.

We introduce x is reducible as an antonym for x is irreducible.

Note that there exists an element of R which is non prime and there exists an element of $\mathbb{Z}^{\mathrm{R}}$ which is prime.

Let R be a right unital, non empty double loop structure. Let us observe that every element of R which is prime is also non zero and non unital and every element of R which is irreducible is also non zero and non unital.

Let R be an integral domain. Observe that every element of R which is prime is also irreducible.

Let F be a field. Let us note that every element of F is reducible.

Let R be a right unital, non empty double loop structure. The functor $\mathrm{IRR}(R)$ yielding a subset of R is defined by the term

(Def. 10) $\{x$, where x is an element of $R : x$ is irreducible$\}$.

Let F be a field. One can check that $\mathrm{IRR}(F)$ is empty.

Now we state the propositions:

(22) Let us consider an integral domain R, a non zero element c of R, and elements b, a, d of R. Suppose $a \cdot b$ is associated to $c \cdot d$ and a is associated to c. Then b is associated to d.

(23) Let us consider an integral domain R, and elements a, b of R. Suppose a is irreducible and b is associated to a. Then b is irreducible.

Let us consider a non degenerated commutative ring R and a non zero element a of R. Now we state the propositions:

(24) a is prime if and only if $\{a\}$–ideal is prime. The theorem is a consequence of (18).

(25) If $\{a\}$–ideal is maximal, then a is irreducible. The theorem is a consequence of (19) and (18).

5. Principal Ideal Domains and Factorial Rings

Note that every field is PID and there exists a non empty double loop structure which is PID.

A principal ideal domain is a PID integral domain. Now we state the proposition:

(26) Let us consider a principal ideal domain R, and a non zero element a of R. Then $\{a\}$–ideal is maximal if and only if a is irreducible. The theorem is a consequence of (19), (20), (18), and (25).

Let R be a principal ideal domain. Observe that every element of R which is irreducible is also prime and every commutative ring which is Euclidean is also PID.

Let R be a principal ideal domain. One can verify that every chain of Ideals R which is ascending is also stagnating.

Let R be a right unital, non empty double loop structure, x be an element of R, and F be a non empty finite sequence of elements of R. We say that F is a factorization of x if and only if

(Def. 11) $x = \prod F$ and for every element i of $\operatorname{dom} F$, $F(i)$ is irreducible.

We say that x is factorizable if and only if

(Def. 12) there exists a non empty finite sequence F of elements of R such that F is a factorization of x.

Assume x is factorizable.

A factorization of x is a non empty finite sequence of elements of R and is defined by

(Def. 13) *it* is a factorization of x.

We say that x is uniquely factorizable if and only if

(Def. 14) x is factorizable and for every factorizations F, G of x, there exists a function B from $\operatorname{dom} F$ into $\operatorname{dom} G$ such that B is bijective and for every element i of $\operatorname{dom} F$, $G(B(i))$ is associated to $F(i)$.

One can verify that every element of R which is uniquely factorizable is also factorizable.

Let R be an integral domain. Let us observe that every element of R which is factorizable is also non zero and non unital.

Let R be a right unital, non empty double loop structure. Let us note that every element of R which is irreducible is also factorizable.

Now we state the propositions:

(27) Let us consider a right unital, non empty double loop structure R, and an element a of R. Then a is irreducible if and only if $\langle a \rangle$ is a factorization of a.

(28) Let us consider a well unital, associative, non empty double loop structure R, elements a, b of R, and non empty finite sequences F, G of elements of R. Suppose F is a factorization of a and G is a factorization of b. Then $F \frown G$ is a factorization of $a \cdot b$.

Let R be a principal ideal domain. Observe that every element of R which is factorizable is also uniquely factorizable.

Let R be a non degenerated ring. We say that R is factorial if and only if

(Def. 15) for every non zero element a of R such that a is a non-unit of R holds a is uniquely factorizable.

One can check that there exists a non degenerated ring which is factorial.

Let R be a factorial, non degenerated ring. Note that every element of R which is non zero and non unital is also factorizable.

A factorial ring is a factorial, non degenerated ring. One can check that every integral domain which is PID is also factorial.

6. Polynomial Rings over Fields

Let L be a field and p be a polynomial of L. The functor $\deg* p$ yielding a natural number is defined by the term

(Def. 16) $\begin{cases} \deg p, & \textbf{if } p \neq \mathbf{0}.L, \\ 0, & \textbf{otherwise}. \end{cases}$

The functor $\deg* L$ yielding a function from Polynom-Ring L into $\mathbb{N}$ is defined by

(Def. 17) for every polynomial p of L, $it(p) = \deg* p$.

Now we state the propositions:

(29) Let us consider a field L, a polynomial p of L, and a non zero polynomial q of L. Then $\deg(p \bmod q) < \deg q$.

(30) Let us consider a field L, an element p of Polynom-Ring L, and a non zero element q of Polynom-Ring L. Then there exist elements u, r of Polynom-Ring L such that

(i) $p = u \cdot q + r$, and

(ii) $r = 0_{\text{Polynom-Ring}\,L}$ or $(\deg* L)(r) < (\deg* L)(q)$.

The theorem is a consequence of (29).

Let L be a field. One can check that Polynom-Ring L is Euclidean.

Note that the functor $\deg* L$ yields a DegreeFunction of Polynom-Ring L.

References

[1] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

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

[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

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

[6] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 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] Nathan Jacobson. *Basic Algebra I.* 2nd edition. Dover Publications Inc., 2009.

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

[14] Artur Korniłowicz. Quotient rings. *Formalized Mathematics*, 13(**4**):573–576, 2005.

[15] Jarosław Kotowicz. Quotient vector spaces and functionals. *Formalized Mathematics*, 11 (**1**):59–68, 2003.

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

[17] Heinz Lüneburg. *Die grundlegenden Strukturen der Algebra (in German).* Oldenbourg Wisenschaftsverlag, 1999.

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

[19] Michał Muzalewski. Opposite rings, modules and their morphisms. *Formalized Mathematics*, 3(**1**):57–65, 1992.

[20] Michał Muzalewski. Category of rings. *Formalized Mathematics*, 2(**5**):643–648, 1991.

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

[22] Michał Muzalewski and Wojciech Skaba. From loops to Abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.

[23] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[24] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.

[25] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.

[26] 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.

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

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

[29] Christoph Schwarzweller. Introduction to rational functions. *Formalized Mathematics*, 20 (**2**):181–191, 2012. doi:10.2478/v10037-012-0021-1.

[30] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Schur's theorem on the stability of networks. *Formalized Mathematics*, 14(**4**):135–142, 2006. doi:10.2478/v10037-006-0017-9.

[31] Yasunari Shidama, Hikofumi Suzuki, and Noboru Endou. Banach algebra of bounded

functionals. *Formalized Mathematics*, 16(**2**):115–122, 2008. doi:10.2478/v10037-008-0017-z.

[32] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.

[33] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

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

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

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

[37] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.

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

[39] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.

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

[41] B.L. van der Waerden. *Algebra I*. 4th edition. Springer, 2003.

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

[43] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 29, 2014