FORMALIZED MATHEMATICS
Volume 3, Number 1, 1992
Université Catholique de Louvain

Opposite Rings, Modules and their Morphisms

Michał Muzalewski
Warsaw University
Białystok

Summary. Let $\mathbb{K} = \langle S; K, 0, 1, +, \cdot \rangle$ be a ring. The structure ${}^{\rm op}\mathbb{K} = \langle S; K, 0, 1, +, \bullet \rangle$ is called anti-ring, if $\alpha \bullet \beta = \beta \cdot \alpha$ for elements α, β of K [12, pages 5–7]. It is easily seen that ${}^{\rm op}\mathbb{K}$ is also a ring. If V is a left module over $\mathbb{K}$, then V is a right module over ${}^{\rm op}\mathbb{K}$. If W is a right module over $\mathbb{K}$, then W is a left module over ${}^{\rm op}\mathbb{K}$. Let K, L be rings. A morphism $J : K \longrightarrow L$ is called anti-homomorphism, if $J(\alpha \cdot \beta) = J(\beta) \cdot J(\alpha)$ for elements α, β of K. If $J : K \longrightarrow L$ is a homomorphism, then $J : K \longrightarrow {}^{\rm op}L$ is an anti-homomorphism. Let K, L be rings, V, W left modules over K, L respectively and $J : K \longrightarrow L$ an anti-monomorphism. A map $f : V \longrightarrow W$ is called J - semilinear, if $f(x + y) = f(x) + f(y)$ and $f(\alpha \cdot x) = J(\alpha) \cdot f(x)$ for vectors x, y of V and a scalar α of K.

MML Identifier: MOD_4.

The papers [19], [18], [21], [3], [4], [1], [20], [17], [2], [7], [8], [11], [14], [15], [16], [5], [6], [9], [13], and [10] provide the notation and terminology for this paper.

1. Opposite functions

In the sequel A, B, C are non-empty sets and f is a function from $[\![A, B]\!]$ into C. Let us consider A, B, C, f. Then $\curvearrowleft f$ is a function from $[\![B, A]\!]$ into C.

We now state the proposition

(1) For every element x of A and for every element y of B holds $f(x, y) = (\curvearrowleft f)(y, x)$.

ISSN 0777–4028

2. Opposite rings

In the sequel K, L will be field structures. Let us consider K. The functor ${}^{\rm op}K$ yielding a strict field structure is defined by:

(Def.1) ${}^{\rm op}K = \langle$the carrier of $K, \curvearrowleft$(the multiplication of K), the addition of K, the reverse-map of K, the unity of K, the zero of $K\rangle$.

We now state four propositions:

(2) The group structure of ${}^{\rm op}K$ = the group structure of K and for an arbitrary x holds x is a scalar of ${}^{\rm op}K$ if and only if x is a scalar of K.

(3) ${}^{\rm op}({}^{\rm op}K)$ = the field structure of K.

(4) (i) $0_K = 0_{{}^{\rm op}K}$,

(ii) $1_K = 1_{{}^{\rm op}K}$,

(iii) for all scalars x, y, z, u of K and for all scalars a, b, c, d of ${}^{\rm op}K$ such that $x = a$ and $y = b$ and $z = c$ and $u = d$ holds $x+y = a+b$ and $x \cdot y = b \cdot a$ and $-x = -a$ and $x + y + z = a + b + c$ and $x + (y + z) = a + (b + c)$ and $(x \cdot y) \cdot z = c \cdot (b \cdot a)$ and $x \cdot (y \cdot z) = (c \cdot b) \cdot a$ and $x \cdot (y + z) = (b + c) \cdot a$ and $(y + z) \cdot x = a \cdot (b + c)$ and $x \cdot y + z \cdot u = b \cdot a + d \cdot c$.

(5) For every ring K holds ${}^{\rm op}K$ is a strict ring.

Let K be a ring. Then ${}^{\rm op}K$ is a strict ring.

One can prove the following proposition

(6) For every associative ring K holds ${}^{\rm op}K$ is an associative ring.

Let K be an associative ring. Then ${}^{\rm op}K$ is a strict associative ring.

Next we state the proposition

(7) For every skew field K holds ${}^{\rm op}K$ is a skew field.

Let K be a skew field. Then ${}^{\rm op}K$ is a strict skew field.

One can prove the following proposition

(8) For every field K holds ${}^{\rm op}K$ is a strict field.

Let K be a field. Then ${}^{\rm op}K$ is a strict field.

3. Opposite modules

In the sequel V denotes a left module structure over K. Let us consider K, V. The functor ${}^{\rm op}V$ yields a strict right module structure over ${}^{\rm op}K$ and is defined as follows:

(Def.2) for every function o from [: the carrier of V, the carrier of ${}^{\rm op}K$:] into the carrier of V such that $o = \curvearrowleft$(the left multiplication of V) holds ${}^{\rm op}V = \langle$the carrier of V, the addition of V, the reverse-map of V, the zero of $V, o\rangle$.

The following proposition is true

(9) The group structure of ${}^{\rm op}V$ = the group structure of V and for an arbitrary x holds x is a vector of V if and only if x is a vector of ${}^{\rm op}V$.

Let us consider K, V, and let o be a function from $[\!:$the carrier of K, the carrier of $V:\!]$ into the carrier of V. The functor ${}^{\rm op}o$ yields a function from $[\!:$the carrier of ${}^{\rm op}V$, the carrier of ${}^{\rm op}K:\!]$ into the carrier of ${}^{\rm op}V$ and is defined by:

(Def.3) ${}^{\rm op}o = \curvearrowleft o$.

One can prove the following two propositions:

(10) The right multiplication of ${}^{\rm op}V = {}^{\rm op}$(the left multiplication of V).

(11) ${}^{\rm op}V = \langle$the carrier of ${}^{\rm op}V$, the addition of ${}^{\rm op}V$, the reverse-map of ${}^{\rm op}V$, the zero of ${}^{\rm op}V$, ${}^{\rm op}$(the left multiplication of V)$\rangle$.

In the sequel W denotes a right module structure over K. Let us consider K, W. The functor ${}^{\rm op}W$ yields a strict left module structure over ${}^{\rm op}K$ and is defined by:

(Def.4) for every function o from $[\!:$the carrier of ${}^{\rm op}K$, the carrier of $W:\!]$ into the carrier of W such that $o = \curvearrowleft$(the right multiplication of W) holds ${}^{\rm op}W = \langle$the carrier of W, the addition of W, the reverse-map of W, the zero of $W, o\rangle$.

We now state the proposition

(12) The group structure of ${}^{\rm op}W =$ the group structure of W and for an arbitrary x holds x is a vector of W if and only if x is a vector of ${}^{\rm op}W$.

Let us consider K, W, and let o be a function from $[\!:$the carrier of W, the carrier of $K:\!]$ into the carrier of W. The functor ${}^{\rm op}o$ yielding a function from $[\!:$the carrier of ${}^{\rm op}K$, the carrier of ${}^{\rm op}W:\!]$ into the carrier of ${}^{\rm op}W$ is defined as follows:

(Def.5) ${}^{\rm op}o = \curvearrowleft o$.

The following propositions are true:

(13) The left multiplication of ${}^{\rm op}W = {}^{\rm op}$(the right multiplication of W).

(14) ${}^{\rm op}W = \langle$the carrier of ${}^{\rm op}W$, the addition of ${}^{\rm op}W$, the reverse-map of ${}^{\rm op}W$, the zero of ${}^{\rm op}W$, ${}^{\rm op}$(the right multiplication of W)$\rangle$.

(15) For every function o from $[\!:$the carrier of K, the carrier of $V:\!]$ into the carrier of V holds ${}^{\rm op}({}^{\rm op}o) = o$.

(16) For every function o from $[\!:$the carrier of K, the carrier of $V:\!]$ into the carrier of V and for every scalar x of K and for every scalar y of ${}^{\rm op}K$ and for every vector v of V and for every vector w of ${}^{\rm op}V$ such that $x = y$ and $v = w$ holds $({}^{\rm op}o)(w, y) = o(x, v)$.

(17) Let K, L be rings. Then for every V being a left module structure over K and for every W being a right module structure over L and for every scalar x of K and for every scalar y of L and for every vector v of V and for every vector w of W such that $L = {}^{\rm op}K$ and $W = {}^{\rm op}V$ and $x = y$ and $v = w$ holds $w \cdot y = x \cdot v$.

(18) For all rings K, L and for every V being a left module structure over K and for every W being a right module structure over L and for all vectors v_1, v_2 of V and for all vectors w_1, w_2 of W such that $L = {}^{\rm op}K$ and $W = {}^{\rm op}V$ and $v_1 = w_1$ and $v_2 = w_2$ holds $w_1 + w_2 = v_1 + v_2$.

(19) For every function o from $[:$the carrier of W, the carrier of $K:]$ into the carrier of W holds ${}^{\mathrm{op}}({}^{\mathrm{op}}o) = o$.

(20) For every function o from $[:$the carrier of W, the carrier of $K:]$ into the carrier of W and for every scalar x of K and for every scalar y of ${}^{\mathrm{op}}K$ and for every vector v of W and for every vector w of ${}^{\mathrm{op}}W$ such that $x = y$ and $v = w$ holds $({}^{\mathrm{op}}o)(y, w) = o(v, x)$.

(21) Let K, L be rings. Then for every V being a left module structure over K and for every W being a right module structure over L and for every scalar x of K and for every scalar y of L and for every vector v of V and for every vector w of W such that $K = {}^{\mathrm{op}}L$ and $V = {}^{\mathrm{op}}W$ and $x = y$ and $v = w$ holds $w \cdot y = x \cdot v$.

(22) For all rings K, L and for every V being a left module structure over K and for every W being a right module structure over L and for all vectors v_1, v_2 of V and for all vectors w_1, w_2 of W such that $K = {}^{\mathrm{op}}L$ and $V = {}^{\mathrm{op}}W$ and $v_1 = w_1$ and $v_2 = w_2$ holds $w_1 + w_2 = v_1 + v_2$.

(23) For every K being a strict field structure and for every V being a left module structure over K holds ${}^{\mathrm{op}}({}^{\mathrm{op}}V) =$ the left module structure of V.

(24) For every K being a strict field structure and for every W being a right module structure over K holds ${}^{\mathrm{op}}({}^{\mathrm{op}}W) =$ the right module structure of W.

(25) For every associative ring K and for every left module V over K holds ${}^{\mathrm{op}}V$ is a strict right module over ${}^{\mathrm{op}}K$.

Let K be an associative ring, and let V be a left module over K. Then ${}^{\mathrm{op}}V$ is a strict right module over ${}^{\mathrm{op}}K$.

One can prove the following proposition

(26) For every associative ring K and for every right module W over K holds ${}^{\mathrm{op}}W$ is a strict left module over ${}^{\mathrm{op}}K$.

Let K be an associative ring, and let W be a right module over K. Then ${}^{\mathrm{op}}W$ is a strict left module over ${}^{\mathrm{op}}K$.

4. Morphisms of rings

We now define several new attributes. Let us consider K, L. A map from K into L is antilinear if:

(Def.6) for all scalars x, y of K holds $\mathrm{it}(x+y) = \mathrm{it}(x) + \mathrm{it}(y)$ and for all scalars x, y of K holds $\mathrm{it}(x \cdot y) = \mathrm{it}(y) \cdot \mathrm{it}(x)$ and $\mathrm{it}(1_K) = 1_L$.

A map from K into L is monomorphism if:

(Def.7) it is linear and it is one-to-one.

A map from K into L is antimonomorphism if:

(Def.8) it is antilinear and it is one-to-one.

A map from K into L is epimorphism if:

(Def.9) it is linear and rng it = the carrier of L.

A map from K into L is antiepimorphism if:

(Def.10) it is antilinear and rng it = the carrier of L.

A map from K into L is isomorphism if:

(Def.11) it is monomorphism and rng it = the carrier of L.

A map from K into L is antiisomorphism if:

(Def.12) it is antimonomorphism and rng it = the carrier of L.

In the sequel J denotes a map from K into K. We now define four new attributes. Let us consider K. A map from K into K is endomorphism if:

(Def.13) it is linear.

A map from K into K is antiendomorphism if:

(Def.14) it is antilinear.

A map from K into K is automorphism if:

(Def.15) it is isomorphism.

A map from K into K is antiautomorphism if:

(Def.16) it is antiisomorphism.

One can prove the following propositions:

(27) J is automorphism if and only if the following conditions are satisfied:
- (i) for all scalars x, y of K holds $J(x+y) = J(x) + J(y)$,
- (ii) for all scalars x, y of K holds $J(x \cdot y) = J(x) \cdot J(y)$,
- (iii) $J(1_K) = 1_K$,
- (iv) J is one-to-one,
- (v) $\operatorname{rng} J$ = the carrier of K.

(28) J is antiautomorphism if and only if the following conditions are satisfied:
- (i) for all scalars x, y of K holds $J(x+y) = J(x) + J(y)$,
- (ii) for all scalars x, y of K holds $J(x \cdot y) = J(y) \cdot J(x)$,
- (iii) $J(1_K) = 1_K$,
- (iv) J is one-to-one,
- (v) $\operatorname{rng} J$ = the carrier of K.

(29) id_K is automorphism.

We follow the rules: K, L will denote rings, J will denote a map from K into L, and x, y will denote scalars of K. Next we state three propositions:

(30) If J is linear, then $J(0_K) = 0_L$ and $J(-x) = -J(x)$ and $J(x-y) = J(x) - J(y)$.

(31) If J is antilinear, then $J(0_K) = 0_L$ and $J(-x) = -J(x)$ and $J(x-y) = J(x) - J(y)$.

(32) For every associative ring K holds id_K is antiautomorphism if and only if K is a commutative ring.

One can prove the following proposition

(33) For every skew field K holds id_K is antiautomorphism if and only if K is a field.

5. Opposite morphisms to morphisms of rings

In the sequel K, L will be field structures and J will be a map from K into L. Let us consider K, L, J. The functor ${}^{\mathrm{op}}J$ yielding a map from K into ${}^{\mathrm{op}}L$ is defined by:

(Def.17) ${}^{\mathrm{op}}J = J$.

Next we state several propositions:

(34) ${}^{\mathrm{op}}({}^{\mathrm{op}}J) = J$.

(35) J is linear if and only if ${}^{\mathrm{op}}J$ is antilinear.

(36) J is antilinear if and only if ${}^{\mathrm{op}}J$ is linear.

(37) J is monomorphism if and only if ${}^{\mathrm{op}}J$ is antimonomorphism.

(38) J is antimonomorphism if and only if ${}^{\mathrm{op}}J$ is monomorphism.

(39) J is epimorphism if and only if ${}^{\mathrm{op}}J$ is antiepimorphism.

(40) J is antiepimorphism if and only if ${}^{\mathrm{op}}J$ is epimorphism.

(41) J is isomorphism if and only if ${}^{\mathrm{op}}J$ is antiisomorphism.

(42) J is antiisomorphism if and only if ${}^{\mathrm{op}}J$ is isomorphism.

In the sequel J will be a map from K into K. We now state four propositions:

(43) J is endomorphism if and only if ${}^{\mathrm{op}}J$ is antilinear.

(44) J is antiendomorphism if and only if ${}^{\mathrm{op}}J$ is linear.

(45) J is automorphism if and only if ${}^{\mathrm{op}}J$ is antiisomorphism.

(46) J is antiautomorphism if and only if ${}^{\mathrm{op}}J$ is isomorphism.

6. Morphisms of groups

In the sequel G, H will denote groups. Let us consider G, H. A map from G into H is said to be a homomorphism from G to H if:

(Def.18) for all elements x, y of G holds $\mathrm{it}(x+y) = \mathrm{it}(x) + \mathrm{it}(y)$.

Then $\mathrm{zero}(G, H)$ is a homomorphism from G to H.

In the sequel f is a homomorphism from G to H. We now define four new constructions. Let us consider G, H. A homomorphism from G to H is monomorphism if:

(Def.19) it is one-to-one.

A homomorphism from G to H is epimorphism if:

(Def.20) $\mathrm{rng}\,\mathrm{it} =$ the carrier of H.

A homomorphism from G to H is isomorphism if:

(Def.21) it is one-to-one and rng it = the carrier of H.

Let us consider G. An endomorphism of G is a homomorphism from G to G.

We now state the proposition

(47) For every element x of G holds $\mathrm{id}_G(x) = x$.

We now define two new constructions. Let us consider G. An endomorphism of G is automorphism-like if:

(Def.22) it is isomorphism.

An automorphism of G is an automorphism-like endomorphism of G.

Then id_G is an automorphism of G.

In the sequel x, y will be elements of G. We now state the proposition

(48) $f(0_G) = 0_H$ and $f(-x) = -f(x)$ and $f(x -' y) = f(x) -' f(y)$.

We adopt the following convention: G, H denote Abelian groups, f denotes a homomorphism from G to H, and x, y denote elements of G. The following proposition is true

(49) $f(x - y) = f(x) - f(y)$.

7. Semilinear morphisms

For simplicity we adopt the following rules: K, L are associative rings, J is a map from K into L, V is a left module over K, and W is a left module over L. Let us consider K, L, J, V, W. A map from V into W is said to be a homomorphism from V to W by J if:

(Def.23) for all vectors x, y of V holds $\mathrm{it}(x + y) = \mathrm{it}(x) + \mathrm{it}(y)$ and for every scalar a of K and for every vector x of V holds $\mathrm{it}(a \cdot x) = J(a) \cdot \mathrm{it}(x)$.

The following proposition is true

(50) $\mathrm{zero}(V, W)$ is a homomorphism from V to W by J.

In the sequel f denotes a homomorphism from V to W by J. We now define three new predicates. Let us consider K, L, J, V, W, f. We say that f is a monomorphism wrp J if and only if:

(Def.24) f is one-to-one.

We say that f is a epimorphism wrp J if and only if:

(Def.25) $\mathrm{rng}\, f$ = the carrier of W.

We say that f is a isomorphism wrp J if and only if:

(Def.26) f is one-to-one and $\mathrm{rng}\, f$ = the carrier of W.

In the sequel J will denote a map from K into K and f will denote a homomorphism from V to V by J. We now define two new constructions. Let us consider K, J, V. An endomorphism of J and V is a homomorphism from V to V by J.

Let us consider K, J, V, f. We say that f is a automorphism wrp J if and only if:

(Def.27) f is one-to-one and $\operatorname{rng} f =$ the carrier of V.

In the sequel W is a left module over K. Let us consider K, V, W. A homomorphism from V to W is a homomorphism from V to W by id_K.

Next we state the proposition

(51) For every map f from V into W holds f is a homomorphism from V to W if and only if for all vectors x, y of V holds $f(x+y) = f(x)+f(y)$ and for every scalar a of K and for every vector x of V holds $f(a\cdot x) = a\cdot f(x)$.

We now define five new constructions. Let us consider K, V, W. A homomorphism from V to W is monomorphism if:

(Def.28) it is one-to-one.

A homomorphism from V to W is epimorphism if:

(Def.29) rng it = the carrier of W.

A homomorphism from V to W is isomorphism if:

(Def.30) it is one-to-one and rng it = the carrier of W.

Let us consider K, V. An endomorphism of V is a homomorphism from V to V.

An endomorphism of V is automorphism if:

(Def.31) it is one-to-one and rng it = the carrier of V.

8. Annex

Next we state three propositions:

(52) For every skew field K holds K is a field if and only if for all scalars x, y of K holds $x \cdot y = y \cdot x$.

(53) For every K being a field structure holds K is a field if and only if K is a skew field and for all scalars x, y of K holds $x \cdot y = y \cdot x$.

(54) For every group G and for all elements x, y, z of G such that $x+y = x+z$ holds $y = z$.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Czesław Byliński. Introduction to categories and functors. *Formalized Mathematics*, 1(**2**):409–420, 1990.
[6] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.
[7] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[8] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[9] Michał Muzalewski. Categories of groups. *Formalized Mathematics*, 2(**4**):563–571, 1991.
[10] Michał Muzalewski. Category of rings. *Formalized Mathematics*, 2(**5**):643–648, 1991.
[11] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[12] Michał Muzalewski. *Foundations of Metric-Affine Geometry.* Dział Wydawnictw Filii UW w Białymstoku, Filia UW w Białymstoku, 1990.
[13] Michał Muzalewski. Rings and modules - part II. *Formalized Mathematics*, 2(**4**):579–585, 1991.
[14] Michał Muzalewski and Wojciech Skaba. Groups, rings, left- and right-modules. *Formalized Mathematics*, 2(**2**):275–278, 1991.
[15] 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.
[16] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[17] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[18] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[19] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[20] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received June 22, 1992