JOURNAL OF FORMALIZED MATHEMATICS
Volume 4, Released 1992, Published 2003
Inst. of Computer Science, Univ. of Białystok

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 [8, 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.

WWW: http://mizar.org/JFM/Vol4/mod_4.html

The articles [4], [12], [13], [2], [3], [1], [11], [6], [7], [9], [5], and [10] provide the notation and terminology for this paper.

1. Opposite functions

In this paper 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.

One can prove the following proposition

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

2. Opposite rings

In the sequel K is a non empty double loop structure.

Let us consider K. The functor ${}^{\rm op}K$ yields a strict double loop structure and is defined as follows:

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

Let us consider K. One can check that ${}^{\rm op}K$ is non empty.

Let K be an add-associative right complementable right zeroed non empty double loop structure. Observe that ${}^{\rm op}K$ is add-associative, right zeroed, and right complementable.

One can prove the following propositions:

(2)(i) The loop structure of ${}^{\rm op}K =$ the loop structure of K,

(ii) if K is add-associative, right zeroed, and right complementable, then $\mathrm{comp}\,{}^{\rm op}K = \mathrm{comp}\,K$, and

(iii) for every set x holds x is a scalar of ${}^{\rm op}K$ iff x is a scalar of K.

© Association of Mizar Users

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

(4) Let K be an add-associative right zeroed right complementable non empty double loop structure. Then

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

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

(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. One can check that $^{\rm op}K$ is Abelian, add-associative, right zeroed, right complementable, well unital, and distributive.

One can prove the following proposition

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

Let K be a ring. One can verify that $^{\rm op}K$ is associative.

We now state the proposition

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

Let K be a skew field. One can check that $^{\rm op}K$ is non degenerated, field-like, associative, Abelian, add-associative, right zeroed, right complementable, well unital, and distributive.

One can prove the following proposition

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

Let K be a field. Observe that $^{\rm op}K$ is strict and field-like.

3. Opposite modules

In the sequel V is a non empty vector space 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 by the condition (Def. 2).

(Def. 2) Let o be a function from [: the carrier of V, the carrier of $^{\rm op}K$:] into the carrier of V. Suppose $o = \curvearrowleft$(the left multiplication of V). Then $^{\rm op}V = \langle$the carrier of V, the addition of V, the zero of V, $o\rangle$.

Let us consider K, V. Observe that $^{\rm op}V$ is non empty.

We now state the proposition

(9)(i) The loop structure of $^{\rm op}V =$ the loop structure of V, and

(ii) for every set x holds x is a vector of V iff 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 $^{\rm op}o$ yielding a function from [: the carrier of $^{\rm op}V$, the carrier of $^{\rm op}K$:] into the carrier of $^{\rm op}V$ is defined by:

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

One can prove the following proposition

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

In the sequel W is a non empty right module structure over K.

Let us consider K, W. The functor ${}^{\rm op}W$ yields a strict vector space structure over ${}^{\rm op}K$ and is defined by the condition (Def. 4).

(Def. 4) Let o be a function from [: the carrier of ${}^{\rm op}K$, the carrier of W :] into the carrier of W. Suppose $o = \curvearrowleft$(the right multiplication of W). Then ${}^{\rm op}W = \langle$the carrier of W, the addition of W, the zero of W, $o\rangle$.

Let us consider K, W. One can check that ${}^{\rm op}W$ is non empty.

The following proposition is true

(12)[1] (i) The loop structure of ${}^{\rm op}W =$ the loop structure of W, and

(ii) for every set x holds x is a vector of W iff 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 ${}^{\rm op}o$ yields a function from [: the carrier of ${}^{\rm op}K$, the carrier of ${}^{\rm op}W$:] into the carrier of ${}^{\rm op}W$ and is defined as follows:

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

We now state a number of propositions:

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

(15)[2] 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) Let o be a function from [: the carrier of K, the carrier of V :] into the carrier of V, x be a scalar of K, y be a scalar of ${}^{\rm op}K$, v be a vector of V, and w be a vector of ${}^{\rm op}V$. If $x = y$ and $v = w$, then $({}^{\rm op}o)(w, y) = o(x, v)$.

(17) Let K, L be rings, V be a non empty vector space structure over K, W be a non empty right module structure over L, x be a scalar of K, y be a scalar of L, v be a vector of V, and w be a vector of W. If $L = {}^{\rm op}K$ and $W = {}^{\rm op}V$ and $x = y$ and $v = w$, then $w \cdot y = x \cdot v$.

(18) Let K, L be rings, V be a non empty vector space structure over K, W be a non empty right module structure over L, v_1, v_2 be vectors of V, and w_1, w_2 be vectors of W. If $L = {}^{\rm op}K$ and $W = {}^{\rm op}V$ and $v_1 = w_1$ and $v_2 = w_2$, then $w_1 + w_2 = v_1 + v_2$.

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

(20) Let o be a function from [: the carrier of W, the carrier of K :] into the carrier of W, x be a scalar of K, y be a scalar of ${}^{\rm op}K$, v be a vector of W, and w be a vector of ${}^{\rm op}W$. If $x = y$ and $v = w$, then $({}^{\rm op}o)(y, w) = o(v, x)$.

(21) Let K, L be rings, V be a non empty vector space structure over K, W be a non empty right module structure over L, x be a scalar of K, y be a scalar of L, v be a vector of V, and w be a vector of W. If $K = {}^{\rm op}L$ and $V = {}^{\rm op}W$ and $x = y$ and $v = w$, then $w \cdot y = x \cdot v$.

(22) Let K, L be rings, V be a non empty vector space structure over K, W be a non empty right module structure over L, v_1, v_2 be vectors of V, and w_1, w_2 be vectors of W. If $K = {}^{\rm op}L$ and $V = {}^{\rm op}W$ and $v_1 = w_1$ and $v_2 = w_2$, then $w_1 + w_2 = v_1 + v_2$.

(23) Let K be a strict non empty double loop structure and V be a non empty vector space structure over K. Then ${}^{\rm op}({}^{\rm op}V) =$ the vector space structure of V.

(24) Let K be a strict non empty double loop structure and W be a non empty right module structure over K. Then ${}^{\rm op}({}^{\rm op}W) =$ the right module structure of W.

[1] The proposition (11) has been removed.

[2] The proposition (14) has been removed.

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

Let K be a ring and let V be a left module over K. Observe that ${}^{\rm op}V$ is Abelian, add-associative, right zeroed, right complementable, and right module-like.

The following proposition is true

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

Let K be a ring and let W be a right module over K. Observe that ${}^{\rm op}W$ is Abelian, add-associative, right zeroed, right complementable, and vector space-like.

4. MORPHISMS OF RINGS

Let K, L be non empty double loop structures and let I_1 be a map from K into L. We say that I_1 is antilinear if and only if:

(Def. 6) For all scalars x, y of K holds $I_1(x+y) = I_1(x)+I_1(y)$ and for all scalars x, y of K holds $I_1(x\cdot y) = I_1(y)\cdot I_1(x)$ and $I_1(\mathbf{1}_K) = \mathbf{1}_L$.

Let K, L be non empty double loop structures and let I_1 be a map from K into L. We say that I_1 is monomorphism if and only if:

(Def. 7) I_1 is linear and one-to-one.

We say that I_1 is antimonomorphism if and only if:

(Def. 8) I_1 is antilinear and one-to-one.

Let K, L be non empty double loop structures and let I_1 be a map from K into L. We say that I_1 is epimorphism if and only if:

(Def. 9) I_1 is linear and $\operatorname{rng} I_1 =$ the carrier of L.

We say that I_1 is antiepimorphism if and only if:

(Def. 10) I_1 is antilinear and $\operatorname{rng} I_1 =$ the carrier of L.

Let K, L be non empty double loop structures and let I_1 be a map from K into L. We say that I_1 is isomorphism if and only if:

(Def. 11) I_1 is monomorphism and $\operatorname{rng} I_1 =$ the carrier of L.

We say that I_1 is antiisomorphism if and only if:

(Def. 12) I_1 is antimonomorphism and $\operatorname{rng} I_1 =$ the carrier of L.

In the sequel J is a map from K into K.

Let K be a non empty double loop structure and let I_1 be a map from K into K. We say that I_1 is endomorphism if and only if:

(Def. 13) I_1 is linear.

We say that I_1 is antiendomorphism if and only if:

(Def. 14) I_1 is antilinear.

We say that I_1 is automorphism if and only if:

(Def. 15) I_1 is isomorphism.

We say that I_1 is antiautomorphism if and only if:

(Def. 16) I_1 is antiisomorphism.

Next we state three 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) $J(\mathbf{1}_K) = \mathbf{1}_K$,

(iv) J is one-to-one, and

(v) $\mathrm{rng} J =$ 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) $J(\mathbf{1}_K) = \mathbf{1}_K$,

(iv) J is one-to-one, and

(v) $\mathrm{rng} J =$ the carrier of K.

(29) id_K is automorphism.

We adopt the following rules: K, L denote rings, J denotes a map from K into L, and x, y denote scalars of K.

Next we state four 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 ring K holds id_K is antiautomorphism iff K is a commutative ring.

(33) For every skew field K holds id_K is antiautomorphism iff K is a field.

5. Opposite morphisms to morphisms of rings

Let K, L be non empty double loop structures and let J be a map from K into L. The functor ${}^{\mathrm{op}}J$ yields a map from K into ${}^{\mathrm{op}}L$ and is defined as follows:

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

In the sequel K, L are add-associative right zeroed right complementable non empty double loop structures and J is a map from K into L.

One can prove the following propositions:

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

(35) Let K, L be add-associative right zeroed right complementable non empty double loop structures and J be a map from K into L. Then J is linear if and only if ${}^{\mathrm{op}}J$ is antilinear.

(36) J is antilinear iff ${}^{\mathrm{op}}J$ is linear.

(37) J is monomorphism iff ${}^{\mathrm{op}}J$ is antimonomorphism.

(38) J is antimonomorphism iff ${}^{\mathrm{op}}J$ is monomorphism.

(39) J is epimorphism iff ${}^{\mathrm{op}}J$ is antiepimorphism.

(40) J is antiepimorphism iff ${}^{\mathrm{op}}J$ is epimorphism.

(41) J is isomorphism iff ${}^{\mathrm{op}}J$ is antiisomorphism.

(42) J is antiisomorphism iff ${}^{\rm op}J$ is isomorphism.

In the sequel J denotes a map from K into K.
Next we state four propositions:

(43) J is endomorphism iff ${}^{\rm op}J$ is antilinear.

(44) J is antiendomorphism iff ${}^{\rm op}J$ is linear.

(45) J is automorphism iff ${}^{\rm op}J$ is antiisomorphism.

(46) J is antiautomorphism iff ${}^{\rm op}J$ is isomorphism.

6. MORPHISMS OF GROUPS

In the sequel G, H are 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 $\mathrm{it}(x+y) = \mathrm{it}(x) + \mathrm{it}(y)$.

Let us consider G, H. Then $\mathrm{ZeroMap}(G,H)$ is a homomorphism from G to H.
In the sequel f denotes a homomorphism from G to H.
Let us consider G, H and let I_1 be a homomorphism from G to H. We say that I_1 is monomorphism if and only if:

(Def. 19) I_1 is one-to-one.

Let us consider G, H and let I_1 be a homomorphism from G to H. We say that I_1 is epimorphism if and only if:

(Def. 20) $\mathrm{rng}\, I_1 =$ the carrier of H.

Let us consider G, H and let I_1 be a homomorphism from G to H. We say that I_1 is isomorphism if and only if:

(Def. 21) I_1 is one-to-one and $\mathrm{rng}\, I_1 =$ the carrier of H.

Let us consider G. An endomorphism of G is a homomorphism from G to G.
Let us consider G. Observe that there exists an endomorphism of G which is isomorphism.
Let us consider G. An automorphism of G is an isomorphism endomorphism of G.
Let us consider G. Then id_G is an automorphism of G.
In the sequel x, y denote elements of G.
The following proposition is true

(48)[3] $f(0_G) = 0_H$ 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) $f(x-y) = f(x) - f(y)$.

[3] The proposition (47) has been removed.

7. Semilinear morphisms

For simplicity, we adopt the following convention: K, L are 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 it satisfies the conditions (Def. 23).

(Def. 23)[4] (i) For all vectors x, y of V holds $\mathrm{it}(x+y) = \mathrm{it}(x) + \mathrm{it}(y)$, and

(ii) for every scalar a of K and for every vector x of V holds $\mathrm{it}(a \cdot x) = J(a) \cdot \mathrm{it}(x)$.

Next we state the proposition

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

In the sequel f is a homomorphism from V to W by J.

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 an epimorphism wrp J if and only if:

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

We say that f is an 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 is a map from K into K and f is a homomorphism from V to V by J.

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 an automorphism wrp J if and only if:

(Def. 27) f is one-to-one and $\mathrm{rng}\, f =$ 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.

One can prove the following proposition

(51) Let f be a map from V into W. Then f is a homomorphism from V to W if and only if the following conditions are satisfied:

(i) for all vectors x, y of V holds $f(x+y) = f(x) + f(y)$, and

(ii) for every scalar a of K and for every vector x of V holds $f(a \cdot x) = a \cdot f(x)$.

Let us consider K, V, W and let I_1 be a homomorphism from V to W. We say that I_1 is monomorphism if and only if:

(Def. 28) I_1 is one-to-one.

We say that I_1 is epimorphism if and only if:

(Def. 29) $\mathrm{rng}\, I_1 =$ the carrier of W.

We say that I_1 is isomorphism if and only if:

(Def. 30) I_1 is one-to-one and $\mathrm{rng}\, I_1 =$ the carrier of W.

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

Let us consider K, V and let I_1 be an endomorphism of V. We say that I_1 is automorphism if and only if:

(Def. 31) I_1 is one-to-one and $\mathrm{rng}\, I_1 =$ the carrier of V.

[4] The definition (Def. 22) has been removed.

REFERENCES

[1] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/binop_1.html.

[2] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[3] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[4] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/zfmisc_1.html.

[5] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/funct_4.html.

[6] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/vectsp_1.html.

[7] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/vectsp_2.html.

[8] Michał Muzalewski. *Foundations of Metric-Affine Geometry*. Dział Wydawnictw Filii UW w Białymstoku, Filia UW w Białymstoku, 1990.

[9] Michał Muzalewski. Categories of groups. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/grcat_1.html.

[10] Michał Muzalewski. Category of rings. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/ringcat1.html.

[11] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/rlvect_1.html.

[12] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

[13] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

Received June 22, 1992

Published January 2, 2004