JOURNAL OF FORMALIZED MATHEMATICS
Volume 3, Released 1991, Published 2003
Inst. of Computer Science, Univ. of Białystok

Rings and Modules — Part II

Michał Muzalewski
Warsaw University
Białystok

Summary. We define the trivial left module, morphism of left modules and the field Z_3. We prove some elementary facts.

MML Identifier: MOD_2.

WWW: http://mizar.org/JFM/Vol3/mod_2.html

The articles [12], [11], [5], [14], [3], [4], [1], [13], [6], [8], [10], [7], [9], and [2] provide the notation and terminology for this paper.

For simplicity, we use the following convention: x, y, z denote sets, D, D' denote non empty sets, R denotes a ring, G, H, S denote non empty vector space structures over R, and U_1 denotes a universal class.

Let us consider R. The functor ${}_R\Theta$ yields a strict left module over R and is defined as follows:

(Def. 2)[1] ${}_R\Theta = \langle \{\emptyset\}, \mathrm{op}_2, \mathrm{op}_0, \pi_2((\text{the carrier of } R) \times \{\emptyset\}) \rangle$.

Next we state the proposition

(1) For every vector x of ${}_R\Theta$ holds $x = 0_{{}_R\Theta}$.

Let R be a non empty double loop structure, let G, H be non empty vector space structures over R, and let f be a map from G into H. We say that f is linear if and only if the conditions (Def. 5) are satisfied.

(Def. 5)[2](i) For all vectors x, y of G holds $f(x+y) = f(x) + f(y)$, and

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

Next we state two propositions:

(4)[3] For every map f from G into H such that f is linear holds f is additive.

(6)[4] Let f be a map from G into H and g be a map from H into S. If f is linear and g is linear, then $g \cdot f$ is linear.

In the sequel R denotes a ring and G, H denote left modules over R.

The following proposition is true

(8)[5] ZeroMap(G, H) is linear.

---

[1] The definition (Def. 1) has been removed.
[2] The definitions (Def. 3) and (Def. 4) have been removed.
[3] The propositions (2) and (3) have been removed.
[4] The proposition (5) has been removed.
[5] The proposition (7) has been removed.

In the sequel G_1, G_2, G_3 are left modules over R.

Let us consider R. We consider left module morphism structures over R as systems
⟨ a dom-map, a cod-map, a `Fun` ⟩,
where the dom-map and the cod-map are left modules over R and the `Fun` is a map from the dom-map into the cod-map.

In the sequel f is a left module morphism structure over R.

Let us consider R, f. The functor $\operatorname{dom} f$ yielding a left module over R is defined by:

(Def. 6) $\operatorname{dom} f =$ the dom-map of f.

The functor $\operatorname{cod} f$ yields a left module over R and is defined by:

(Def. 7) $\operatorname{cod} f =$ the cod-map of f.

Let us consider R, f. The functor $\operatorname{fun} f$ yields a map from $\operatorname{dom} f$ into $\operatorname{cod} f$ and is defined by:

(Def. 8) $\operatorname{fun} f =$ the `Fun` of f.

We now state the proposition

(9) For every map f_0 from G_1 into G_2 such that $f = \langle G_1, G_2, f_0 \rangle$ holds $\operatorname{dom} f = G_1$ and $\operatorname{cod} f = G_2$ and $\operatorname{fun} f = f_0$.

Let us consider R, G, H. The functor $\mathrm{ZERO}(G,H)$ yields a strict left module morphism structure over R and is defined by:

(Def. 9) $\mathrm{ZERO}(G,H) = \langle G, H, \mathrm{ZeroMap}(G,H) \rangle$.

Let us consider R and let I_1 be a left module morphism structure over R. We say that I_1 is left module morphism-like if and only if:

(Def. 10) $\operatorname{fun} I_1$ is linear.

Let us consider R. Note that there exists a left module morphism structure over R which is strict and left module morphism-like.

Let us consider R. A left module morphism of R is a left module morphism-like left module morphism structure over R.

Next we state the proposition

(10) For every left module morphism F of R holds the `Fun` of F is linear.

Let us consider R, G, H. Observe that $\mathrm{ZERO}(G,H)$ is left module morphism-like.

Let us consider R, G, H. A left module morphism of R is said to be a morphism from G to H if:

(Def. 11) $\operatorname{dom} \mathrm{it} = G$ and $\operatorname{cod} \mathrm{it} = H$.

Let us consider R, G, H. Note that there exists a morphism from G to H which is strict.

We now state three propositions:

(11) Let f be a left module morphism structure over R. If $\operatorname{dom} f = G$ and $\operatorname{cod} f = H$ and $\operatorname{fun} f$ is linear, then f is a morphism from G to H.

(12) For every map f from G into H such that f is linear holds $\langle G, H, f \rangle$ is a strict morphism from G to H.

(13) id_G is linear.

Let us consider R, G. The functor I_G yields a strict morphism from G to G and is defined by:

(Def. 12) $\mathrm{I}_G = \langle G, G, \mathrm{id}_G \rangle$.

Let us consider R, G, H. Then $\mathrm{ZERO}(G,H)$ is a strict morphism from G to H.

The following propositions are true:

(14) Let F be a morphism from G to H. Then there exists a map f from G into H such that the left module morphism structure of $F = \langle G, H, f\rangle$ and f is linear.

(15) For every strict morphism F from G to H there exists a map f from G into H such that $F = \langle G, H, f\rangle$.

(16) For every left module morphism F of R there exist G, H such that F is a morphism from G to H.

(17) Let F be a strict left module morphism of R. Then there exist left modules G, H over R and there exists a map f from G into H such that F is a strict morphism from G to H and $F = \langle G, H, f\rangle$ and f is linear.

(18) Let g, f be left module morphisms of R. Suppose $\operatorname{dom} g = \operatorname{cod} f$. Then there exist G_1, G_2, G_3 such that g is a morphism from G_2 to G_3 and f is a morphism from G_1 to G_2.

Let us consider R and let G, F be left module morphisms of R. Let us assume that $\operatorname{dom} G = \operatorname{cod} F$. The functor $G \cdot F$ yielding a strict left module morphism of R is defined by the condition (Def. 13).

(Def. 13) Let G_1, G_2, G_3 be left modules over R, g be a map from G_2 into G_3, and f be a map from G_1 into G_2. Suppose the left module morphism structure of $G = \langle G_2, G_3, g\rangle$ and the left module morphism structure of $F = \langle G_1, G_2, f\rangle$. Then $G \cdot F = \langle G_1, G_3, g \cdot f\rangle$.

Next we state the proposition

(20)[6] Let G be a morphism from G_2 to G_3 and F be a morphism from G_1 to G_2. Then $G \cdot F$ is a strict morphism from G_1 to G_3.

Let us consider R, G_1, G_2, G_3, let G be a morphism from G_2 to G_3, and let F be a morphism from G_1 to G_2. The functor $G * F$ yields a strict morphism from G_1 to G_3 and is defined by:

(Def. 14) $G * F = G \cdot F$.

We now state several propositions:

(21) Let G be a morphism from G_2 to G_3, F be a morphism from G_1 to G_2, g be a map from G_2 into G_3, and f be a map from G_1 into G_2. If $G = \langle G_2, G_3, g\rangle$ and $F = \langle G_1, G_2, f\rangle$, then $G * F = \langle G_1, G_3, g \cdot f\rangle$ and $G \cdot F = \langle G_1, G_3, g \cdot f\rangle$.

(22) Let f, g be strict left module morphisms of R. Suppose $\operatorname{dom} g = \operatorname{cod} f$. Then there exist left modules G_1, G_2, G_3 over R and there exists a map f_0 from G_1 into G_2 and there exists a map g_0 from G_2 into G_3 such that $f = \langle G_1, G_2, f_0\rangle$ and $g = \langle G_2, G_3, g_0\rangle$ and $g \cdot f = \langle G_1, G_3, g_0 \cdot f_0\rangle$.

(23) For all strict left module morphisms f, g of R such that $\operatorname{dom} g = \operatorname{cod} f$ holds $\operatorname{dom}(g \cdot f) = \operatorname{dom} f$ and $\operatorname{cod}(g \cdot f) = \operatorname{cod} g$.

(24) Let G_1, G_2, G_3, G_4 be left modules over R, f be a strict morphism from G_1 to G_2, g be a strict morphism from G_2 to G_3, and h be a strict morphism from G_3 to G_4. Then $h \cdot (g \cdot f) = (h \cdot g) \cdot f$.

(25) For all strict left module morphisms f, g, h of R such that $\operatorname{dom} h = \operatorname{cod} g$ and $\operatorname{dom} g = \operatorname{cod} f$ holds $h \cdot (g \cdot f) = (h \cdot g) \cdot f$.

(26)(i) $\operatorname{dom}(\mathrm{I}_G) = G$,

(ii) $\operatorname{cod}(\mathrm{I}_G) = G$,

(iii) for every strict left module morphism f of R such that $\operatorname{cod} f = G$ holds $\mathrm{I}_G \cdot f = f$, and

(iv) for every strict left module morphism g of R such that $\operatorname{dom} g = G$ holds $g \cdot \mathrm{I}_G = g$.

[6] The proposition (19) has been removed.

Let us consider x, y, z. Observe that $\{x,y,z\}$ is non empty.
One can prove the following three propositions:

(28)[7] For all elements u, v, w of U_1 holds $\{u,v,w\}$ is an element of U_1.

(29) For every element u of U_1 holds $\operatorname{succ} u$ is an element of U_1.

(30) 0 is an element of U_1 and 1 is an element of U_1 and 2 is an element of U_1.

In the sequel a, b are elements of $\{0,1,2\}$.
Let us consider a. The functor $-a$ yielding an element of $\{0,1,2\}$ is defined by:

(Def. 15)(i) $-a = 0$ if $a = 0$,
(ii) $-a = 2$ if $a = 1$,
(iii) $-a = 1$ if $a = 2$.

Let us consider b. The functor $a+b$ yields an element of $\{0,1,2\}$ and is defined as follows:

(Def. 16)(i) $a+b = b$ if $a = 0$,
(ii) $a+b = a$ if $b = 0$,
(iii) $a+b = 2$ if $a = 1$ and $b = 1$,
(iv) $a+b = 0$ if $a = 1$ and $b = 2$,
(v) $a+b = 0$ if $a = 2$ and $b = 1$,
(vi) $a+b = 1$ if $a = 2$ and $b = 2$.

The functor $a \cdot b$ yielding an element of $\{0,1,2\}$ is defined as follows:

(Def. 17)(i) $a \cdot b = 0$ if $b = 0$,
(ii) $a \cdot b = 0$ if $a = 0$,
(iii) $a \cdot b = a$ if $b = 1$,
(iv) $a \cdot b = b$ if $a = 1$,
(v) $a \cdot b = 1$ if $a = 2$ and $b = 2$.

The binary operation add_3 on $\{0,1,2\}$ is defined by:

(Def. 18) $\mathrm{add}_3(a, b) = a+b$.

The binary operation mult_3 on $\{0,1,2\}$ is defined as follows:

(Def. 19) $\mathrm{mult}_3(a, b) = a \cdot b$.

The unary operation compl_3 on $\{0,1,2\}$ is defined as follows:

(Def. 20) $\mathrm{compl}_3(a) = -a$.

The element unit_3 of $\{0,1,2\}$ is defined as follows:

(Def. 21) $\mathrm{unit}_3 = 1$.

The element zero_3 of $\{0,1,2\}$ is defined as follows:

(Def. 22) $\mathrm{zero}_3 = 0$.

The strict double loop structure $\mathbb{Z}_3$ is defined as follows:

(Def. 23) $\mathbb{Z}_3 = \langle \{0,1,2\}, \mathrm{add}_3, \mathrm{mult}_3, \mathrm{unit}_3, \mathrm{zero}_3 \rangle$.

One can verify that $\mathbb{Z}_3$ is non empty.
One can prove the following proposition

[7] The proposition (27) has been removed.

(32)[8](i) $0_{Z_3} = 0$,

(ii) $\mathbf{1}_{Z_3} = 1$,

(iii) 0_{Z_3} is an element of $\{0,1,2\}$,

(iv) $\mathbf{1}_{Z_3}$ is an element of $\{0,1,2\}$,

(v) the addition of $Z_3 = \mathrm{add}_3$, and

(vi) the multiplication of $Z_3 = \mathrm{mult}_3$.

One can check that Z_3 is add-associative, right zeroed, and right complementable.

We now state several propositions:

(33) Let x, y be scalars of Z_3 and X, Y be elements of $\{0,1,2\}$. If $X = x$ and $Y = y$, then $x+y = X+Y$ and $x \cdot y = X \cdot Y$ and $-x = -X$.

(34) Let x, y, z be scalars of Z_3 and X, Y, Z be elements of $\{0,1,2\}$. Suppose $X = x$ and $Y = y$ and $Z = z$. Then $x+y+z = X+Y+Z$ and $x+(y+z) = X+(Y+Z)$ and $x \cdot y \cdot z = X \cdot Y \cdot Z$ and $x \cdot (y \cdot z) = X \cdot (Y \cdot Z)$.

(35) Let x, y, z, a, b be elements of $\{0,1,2\}$. Suppose $a = 0$ and $b = 1$. Then $x+y = y+x$ and $(x+y)+z = x+(y+z)$ and $x+a = x$ and $x+-x = a$ and $x \cdot y = y \cdot x$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ and $b \cdot x = x$ and if $x \neq a$, then there exists an element y of $\{0,1,2\}$ such that $x \cdot y = b$ and $a \neq b$ and $x \cdot (y+z) = x \cdot y + x \cdot z$.

(36) Let F be a non empty double loop structure. Suppose that for all scalars x, y, z of F holds $x+y = y+x$ and $(x+y)+z = x+(y+z)$ and $x+0_F = x$ and $x+-x = 0_F$ and $x \cdot y = y \cdot x$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ and $\mathbf{1}_F \cdot x = x$ and if $x \neq 0_F$, then there exists a scalar y of F such that $x \cdot y = \mathbf{1}_F$ and $0_F \neq \mathbf{1}_F$ and $x \cdot (y+z) = x \cdot y + x \cdot z$. Then F is a field.

(37) Z_3 is a Fanoian field.

One can verify that Z_3 is Fanoian, add-associative, right zeroed, right complementable, Abelian, commutative, associative, left unital, distributive, and field-like.

The following two propositions are true:

(38) For every function f from D into D' such that $D \in U_1$ and $D' \in U_1$ holds $f \in U_1$.

(40)[9](i) The carrier of $Z_3 \in U_1$,

(ii) the addition of Z_3 is an element of U_1,

(iii) $\mathrm{comp} Z_3$ is an element of U_1,

(iv) the zero of Z_3 is an element of U_1,

(v) the multiplication of Z_3 is an element of U_1, and

(vi) the unity of Z_3 is an element of U_1.

REFERENCES

[1] Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal1.html.

[2] Czesław Byliński. Basic functions and operations on functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_3.html.

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

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

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

[8] The proposition (31) has been removed.
[9] The proposition (39) has been removed.

[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. Midpoint algebras. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/midsp_1.html.

[8] 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.

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

[10] Bogdan Nowak and Grzegorz Bancerek. Universal classes. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/classes2.html.

[11] Andrzej Trybulec. Enumerated sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/enumset1.html.

[12] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

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

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

Received October 18, 1991

Published January 2, 2004