FORMALIZED MATHEMATICS
Vol.2, No.4, September–October 1991
Université Catholique de Louvain

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 proof some elementary facts.

MML Identifier: MOD_2.

The terminology and notation used in this paper are introduced in the following articles: [14], [13], [4], [5], [6], [2], [3], [1], [7], [9], [11], [12], [10], and [8]. For simplicity we adopt the following convention: x, y, z are arbitrary, D is a non-empty set, R, R_1, R_2, R_3 are associative rings, G is a left module structure over R, H is a left module structure over R, S is a left module structure over R, G_1 is a left module structure over R_1, G_2 is a left module structure over R_2, G_3 is a left module structure over R_3, and U_1 is a universal class. Let us consider x. Then $\{x\}$ is a non-empty set.

Let us consider R. $\mathrm{lop}(R)$ is a function from $[\!:$ the carrier of R, the carrier of the trivial group $:\!]$ into the carrier of the trivial group.

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

(Def.1) $\quad {}_R\Theta = \langle \text{the trivial group}, \mathrm{lop}(R) \rangle$.

Next we state the proposition

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

Let us consider R_1, R_2, G_1, G_2. A map from G_1 into G_2 is a map from the carrier of G_1 into the carrier of G_2.

Let us consider R_1, R_2, R_3, G_1, G_2, G_3, and let f be a map from G_1 into G_2, and let g be a map from G_2 into G_3. Then $g \cdot f$ is a map from G_1 into G_3.

Let us consider R, G. The functor id_G yielding a map from G into G is defined as follows:

(Def.2) $\quad \mathrm{id}_G = \mathrm{id}_{(\text{the carrier of } G)}$.

ISSN 0777–4028

The following propositions are true:

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

(3) For every map f from G_1 into G_2 holds $f \cdot \mathrm{id}_{G_1} = f$ and $\mathrm{id}_{G_2} \cdot f = f$.

Let us consider R_1, R_2, G_1, G_2. The functor $\mathrm{zero}(G_1, G_2)$ yields a map from G_1 into G_2 and is defined as follows:

(Def.3) $\mathrm{zero}(G_1, G_2) = \mathrm{zero}($ the carrier of G_1, the carrier of $G_2)$.

Let us consider R, and let G, H be left module structures over R, and let f be a map from G into H. We say that f is linear if and only if:

(Def.4) for all vectors x, y of G holds $f(x + y) = f(x) + f(y)$ and for every scalar a of R and for every vector x of G holds $f(a \cdot x) = a \cdot f(x)$.

The following propositions are true:

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

(5) For every map f from G_1 into G_2 and for every map g from G_2 into G_3 and for every vector x of G_1 holds $(g \cdot f)(x) = g(f(x))$.

(6) For every map f from G into H and for every map g from H into S such that f is linear and g is linear holds $g \cdot f$ is linear.

For simplicity we adopt the following rules: R, R_1, R_2 denote associative rings, G denotes a left module over R, H denotes a left module over R, G_1 denotes a left module over R_1, and G_2 denotes a left module over R_2. The following propositions are true:

(7) For every vector x of G_1 holds $(\mathrm{zero}(G_1, G_2))(x) = \Theta_{G_2}$.

(8) $\mathrm{zero}(G, H)$ is linear.

In the sequel G_1 will denote a left module over R, G_2 will denote a left module over R, and G_3 will denote a left module over R. Let us consider R. We consider left module morphism structures over R which are systems

⟨a dom-map, a cod-map, a `Fun`⟩,

where the dom-map, the cod-map are a left module over R and the `Fun` is a map from the dom-map into the cod-map.

In the sequel f will be a left module morphism structure over R. We now define two new functors. Let us consider R, f. The functor $\mathrm{dom}\, f$ yields a left module over R and is defined as follows:

(Def.5) $\mathrm{dom}\, f =$ the dom-map of f.

The functor $\mathrm{cod}\, f$ yields a left module over R and is defined as follows:

(Def.6) $\mathrm{cod}\, f =$ the cod-map of f.

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

(Def.7) $\mathrm{fun}\, f =$ the `Fun` of f.

One can prove the following 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 $\mathrm{dom}\, f = G_1$ and $\mathrm{cod}\, f = G_2$ and $\mathrm{fun}\, f = f_0$.

Let us consider R, G, H. The functor ZERO G yielding a left module morphism structure over R is defined as follows:

(Def.8) ZERO $G = \langle G, H, \mathrm{zero}(G, H) \rangle$.

Let us consider R. A left module morphism structure over R is said to be a left module morphism of R if:

(Def.9) fun it is linear.

One can prove the following proposition

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

Let us consider R, G, H. Then ZERO G is a left module morphism of R.

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

(Def.10) dom it $= G$ and cod it $= H$.

One can prove the following three propositions:

(11) If dom $f = G$ and cod $f = H$ and 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 morphism from G to H.

(13) id_G is linear.

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

(Def.11) $\mathrm{I}_G = \langle G, G, \mathrm{id}_G \rangle$.

Let us consider R, G, H. Then ZERO G is a morphism from G to H.

The following propositions are true:

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

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

(18) For all left module morphisms g, f of R such that dom $g =$ cod f 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.

(19) For every left module morphism F of R holds F is a morphism from dom F to cod F.

Let us consider R, and let G, F be left module morphisms of R. Let us assume that dom $G =$ cod F. The functor $G \cdot F$ yields a left module morphism of R and is defined as follows:

(Def.12) for all left modules G_1, G_2, G_3 over R and for every map g from G_2 into G_3 and for every map f from G_1 into G_2 such that $G = \langle G_2, G_3, g\rangle$ and $F = \langle G_1, G_2, f\rangle$ holds $G \cdot F = \langle G_1, G_3, g \cdot f\rangle$.

Next we state the proposition

(20) For every morphism G from G_2 to G_3 and for every morphism F from G_1 to G_2 holds $G \cdot F$ is a morphism from G_1 to G_3.

Let us consider R, G_1, G_2, G_3, and 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 $F[G]$ yielding a morphism from G_1 to G_3 is defined by:

(Def.13) $F[G] = G \cdot F$.

We now state several propositions:

(21) Let G be a morphism from G_2 to G_3. Then for every morphism F from G_1 to G_2 and for every map g from G_2 into G_3 and for every map f from G_1 into G_2 such that $G = \langle G_2, G_3, g\rangle$ and $F = \langle G_1, G_2, f\rangle$ holds $F[G] = \langle G_1, G_3, g \cdot f\rangle$ and $G \cdot F = \langle G_1, G_3, g \cdot f\rangle$.

(22) Let f, g be left module morphisms of R. Then if $\mathrm{dom}\, g = \mathrm{cod}\, f$, 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 left module morphisms f, g of R such that $\mathrm{dom}\, g = \mathrm{cod}\, f$ holds $\mathrm{dom}(g \cdot f) = \mathrm{dom}\, f$ and $\mathrm{cod}(g \cdot f) = \mathrm{cod}\, g$.

(24) For all left modules G_1, G_2, G_3, G_4 over R and for every morphism f from G_1 to G_2 and for every morphism g from G_2 to G_3 and for every morphism h from G_3 to G_4 holds $h \cdot (g \cdot f) = h \cdot g \cdot f$.

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

(26) $\mathrm{dom}(\mathrm{I}_G) = G$ and $\mathrm{cod}(\mathrm{I}_G) = G$ and for every left module morphism f of R such that $\mathrm{cod}\, f = G$ holds $\mathrm{I}_G \cdot f = f$ and for every left module morphism g of R such that $\mathrm{dom}\, g = G$ holds $g \cdot \mathrm{I}_G = g$.

(27) $\{x, y, z\}$ is a non-empty set.

Let us consider x, y, z. Then $\{x, y, z\}$ is a non-empty set.

We now state four propositions:

(28) 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 $\mathrm{succ}\, u$ is an element of U_1.

(30) $\overline{\mathbf{0}}$ is an element of U_1 and $\overline{\mathbf{1}}$ is an element of U_1 and $\overline{\mathbf{2}}$ is an element of U_1.

(31) $\overline{\mathbf{0}} \neq \overline{\mathbf{1}}$ and $\overline{\mathbf{0}} \neq \overline{\mathbf{2}}$ and $\overline{\mathbf{1}} \neq \overline{\mathbf{2}}$.

In the sequel a, b will be elements of $\{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}\}$. We now define three new functors. Let us consider a. The functor $-a$ yields an element of $\{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}\}$ and is defined as follows:

(Def.14) (i) $-a = \overline{\mathbf{0}}$ if $a = \overline{\mathbf{0}}$,
(ii) $-a = \overline{\mathbf{2}}$ if $a = \overline{\mathbf{1}}$,
(iii) $-a = \overline{\mathbf{1}}$ if $a = \overline{\mathbf{2}}$.

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

(Def.15) (i) $a+b = b$ if $a = \overline{\mathbf{0}}$,
(ii) $a+b = a$ if $b = \overline{\mathbf{0}}$,
(iii) $a+b = \overline{\mathbf{2}}$ if $a = \overline{\mathbf{1}}$ and $b = \overline{\mathbf{1}}$,
(iv) $a+b = \overline{\mathbf{0}}$ if $a = \overline{\mathbf{1}}$ and $b = \overline{\mathbf{2}}$,
(v) $a+b = \overline{\mathbf{0}}$ if $a = \overline{\mathbf{2}}$ and $b = \overline{\mathbf{1}}$,
(vi) $a+b = \overline{\mathbf{1}}$ if $a = \overline{\mathbf{2}}$ and $b = \overline{\mathbf{2}}$.

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

(Def.16) (i) $a \cdot b = \overline{\mathbf{0}}$ if $b = \overline{\mathbf{0}}$,
(ii) $a \cdot b = \overline{\mathbf{0}}$ if $a = \overline{\mathbf{0}}$,
(iii) $a \cdot b = a$ if $b = \overline{\mathbf{1}}$,
(iv) $a \cdot b = b$ if $a = \overline{\mathbf{1}}$,
(v) $a \cdot b = \overline{\mathbf{1}}$ if $a = \overline{\mathbf{2}}$ and $b = \overline{\mathbf{2}}$.

We now define five new functors. The binary operation add_3 on $\{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}\}$ is defined by:

(Def.17) $\mathrm{add}_3(a, b) = a + b$.

The binary operation mult_3 on $\{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}\}$ is defined by:

(Def.18) $\mathrm{mult}_3(a, b) = a \cdot b$.

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

(Def.19) $\mathrm{compl}_3(a) = -a$.

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

(Def.20) $\mathrm{unit}_3 = \overline{\mathbf{1}}$.

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

(Def.21) $\mathrm{zero}_3 = \overline{\mathbf{0}}$.

The field structure Z_3 is defined by:

(Def.22) $\mathrm{Z}_3 = \langle \{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}\}, \mathrm{mult}_3, \mathrm{add}_3, \mathrm{compl}_3, \mathrm{unit}_3, \mathrm{zero}_3 \rangle$.

Next we state several propositions:

(32) $0_{\mathrm{Z}_3} = \overline{\mathbf{0}}$ and $1_{\mathrm{Z}_3} = \overline{\mathbf{1}}$ and 0_{Z_3} is an element of $\{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}\}$ and 1_{Z_3} is an element of $\{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}\}$ and the addition of $\mathrm{Z}_3 = \mathrm{add}_3$ and the multiplication of $\mathrm{Z}_3 = \mathrm{mult}_3$ and the reverse-map of $\mathrm{Z}_3 = \mathrm{compl}_3$.

(33) For all scalars x, y of Z_3 and for all elements X, Y of $\{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}\}$ such that $X = x$ and $Y = y$ holds $x + y = X + Y$ and $x \cdot y = X \cdot Y$ and $-x = -X$.

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

(i) $x + y = y + x$,

(ii) $x + y + z = x + (y + z)$,

(iii) $x + a = x$,

(iv) $x + -x = a$,

(v) $x \cdot y = y \cdot x$,

(vi) $x \cdot y \cdot z = x \cdot (y \cdot z)$,

(vii) $x \cdot b = x$,

(viii) if $x \neq a$, then there exists an element y of $\{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}\}$ such that $x \cdot y = b$,

(ix) $a \neq b$,

(x) $x \cdot (y + z) = x \cdot y + x \cdot z$.

(36) Let F be a field structure. Suppose that

(i) 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 $x \cdot 1_F = x$ but if $x \neq 0_F$, then there exists a scalar y of F such that $x \cdot y = 1_F$ and $0_F \neq 1_F$ and $x \cdot (y + z) = x \cdot y + x \cdot z$.

Then F is a field.

(37) Z_3 is a Fano field.

Let us note that it makes sense to consider the following constant. Then Z_3 is a Fano field.

In the sequel D' is a non-empty set. One can prove the following propositions:

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

(39) For every G being a field structure such that the carrier of $G \in U_1$ holds the addition of G is an element of U_1 and the reverse-map of G is an element of U_1 and the zero of G is an element of U_1 and the multiplication of G is an element of U_1 and the unity of G is an element of U_1.

(40) The carrier of $\mathrm{Z}_3 \in U_1$ and the addition of Z_3 is an element of U_1 and the reverse-map of Z_3 is an element of U_1 and the zero of Z_3 is an element of U_1 and the multiplication of Z_3 is an element of U_1 and the unity of Z_3 is an element of U_1.

References

[1] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.

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

[3] Grzegorz Bancerek. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 1990.

[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

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

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

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

[8] Michał Muzalewski. Categories of groups. *Formalized Mathematics*, 2(**4**):563–571, 1991.

[9] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[10] Michał Muzalewski and Wojciech Skaba. Groups, rings, left- and right-modules. *Formalized Mathematics*, 2(**2**):275–278, 1991.
[11] 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.
[12] Bogdan Nowak and Grzegorz Bancerek. Universal classes. *Formalized Mathematics*, 1(**3**):595–600, 1990.
[13] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[14] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

Received October 18, 1991