

# Ring of Endomorphisms and Modules over a Ring

Yasushige Watase  
Suginami-ku Matsunoki  
3-21-6 Tokyo, Japan

**Summary.** We formalize in the Mizar system [3], [4] some basic properties on left module over a ring such as constructing a module via a ring of endomorphism of an abelian group and the set of all homomorphisms of modules form a module [1] along with Ch. 2 set. 1 of [2].

The formalized items are shown in the below list with notations:  $M_{ab}$  for an Abelian group with a suffix “ $_{ab}$ ” and  $M$  without a suffix is used for left modules over a ring.

1. The endomorphism ring of an abelian group denoted by  $\mathbf{End}(M_{ab})$ .
2. A pair of an Abelian group  $M_{ab}$  and a ring homomorphism  $R \xrightarrow{\rho} \mathbf{End}(M_{ab})$  determines a left  $R$ -module, formalized as a function  $\mathbf{AbGrLMod}(M_{ab}, \rho)$  in the article.
3. The set of all functions from  $M$  to  $N$  form  $R$ -module and denoted by  $\mathbf{Func\_Mod}_R(M, N)$ .
4. The set  $R$ -module homomorphisms of  $M$  to  $N$ , denoted by  $\mathbf{Hom}_R(M, N)$ , forms  $R$ -module.
5. A formal proof of  $\mathbf{Hom}_R(\bar{R}, M) \cong M$  is given, where the  $\bar{R}$  denotes the regular representation of  $R$ , i.e. we regard  $R$  itself as a left  $R$ -module.
6. A formal proof of  $\mathbf{AbGrLMod}(M'_{ab}, \rho') \cong M$  where  $M'_{ab}$  is an abelian group obtained by removing the scalar multiplication from  $M$ , and  $\rho'$  is obtained by currying the scalar multiplication of  $M$ .

The removal of the multiplication from  $M$  has been done by the forgettable functor defined as  $\mathbf{AbGr}$  in the article.

MSC: 13C05 13C60 68V20

Keywords: module; endomorphism ring

MML identifier: LMOD\_XX1, version: 8.1.12 5.71.1431

Let  $M, N$  be Abelian groups. The functor  $\text{ADD}(M, N)$  yielding a binary operation on (the carrier of  $N$ )<sup>(the carrier of  $M$ )</sup> is defined by

(Def. 1) for every elements  $f, g$  of (the carrier of  $N$ ) <sup>$\alpha$</sup> ,  $it(f, g) =$  (the addition of  $N$ ) <sup>$\circ$</sup> ( $f, g$ ), where  $\alpha$  is the carrier of  $M$ .

Now we state the propositions:

- (1) Let us consider Abelian groups  $M, N$ , and elements  $f, g, h$  of (the carrier of  $N$ ) <sup>$\alpha$</sup> . Then  $h = (\text{ADD}(M, N))(f, g)$  if and only if for every element  $x$  of the carrier of  $M$ ,  $h(x) = f(x) + g(x)$ , where  $\alpha$  is the carrier of  $M$ .
- (2) Let us consider Abelian groups  $M, N$ , and homomorphisms  $f, g$  from  $M$  to  $N$ . Then  $(\text{ADD}(M, N))(f, g)$  is a homomorphism from  $M$  to  $N$ . The theorem is a consequence of (1).

Let  $M$  be an Abelian group. The functor  $\text{set\_End}(M)$  yielding a non empty subset of (the carrier of  $M$ )<sup>(the carrier of  $M$ )</sup> is defined by the term

(Def. 2)  $\{f, \text{ where } f \text{ is a function from } M \text{ into } M : f \text{ is an endomorphism of } M\}$ .

The functor  $\text{add\_End}(M)$  yielding a binary operation on  $\text{set\_End}(M)$  is defined by the term

(Def. 3)  $\text{ADD}(M, M) \upharpoonright (\text{set\_End}(M) \times \text{set\_End}(M))$ .

Now we state the proposition:

- (3) Let us consider an Abelian group  $M$ , and endomorphisms  $f, g$  of  $M$ . Then
  - (i)  $f, g \in$  (the carrier of  $M$ ) <sup>$\alpha$</sup> , and
  - (ii)  $(\text{add\_End}(M))(\langle f, g \rangle) = (\text{ADD}(M, M))(f, g)$ , and
  - (iii)  $(\text{ADD}(M, M))(f, g)$  is an endomorphism of  $M$ ,

where  $\alpha$  is the carrier of  $M$ . The theorem is a consequence of (2).

From now on  $M, N$  denote Abelian groups. Let  $M$  be an Abelian group and  $f, g$  be elements of (the carrier of  $M$ )<sup>(the carrier of  $M$ )</sup>. Let us note that the functor  $g \cdot f$  yields an element of (the carrier of  $M$ )<sup>(the carrier of  $M$ )</sup>.

We prepare composition of homomorphisms.

Let  $M$  be an Abelian group. The functor  $\text{FuncComp}(M)$  yielding a binary operation on (the carrier of  $M$ )<sup>(the carrier of  $M$ )</sup> is defined by

(Def. 4) for every elements  $f, g$  of (the carrier of  $M$ ) <sup>$\alpha$</sup> ,  $it(f, g) = f \cdot g$ , where  $\alpha$  is the carrier of  $M$ .

- (4) Let us consider Abelian groups  $M, N$ , and elements  $f, g$  of (the carrier of  $N$ ) <sup>$\alpha$</sup> . Then  $(\text{ADD}(M, N))(f, g) = (\text{ADD}(M, N))(g, f)$ , where  $\alpha$  is the carrier of  $M$ . The theorem is a consequence of (1).

(5) ENDOMORPHISM OF  $M$  IS CLOSED UNDER COMPOSITION:

Let us consider an Abelian group  $M$ , and endomorphisms  $f, g$  of  $M$ . Then  $(\text{FuncComp}(M))(f, g)$  is an endomorphism of  $M$ .

PROOF: Reconsider  $F = (\text{FuncComp}(M))(f, g)$  as an element of (the carrier of  $M$ )<sup>(the carrier of  $M$ )</sup>.  $F$  is additive.  $\square$

Let  $M$  be an Abelian group. The functor  $\text{mult\_End}(M)$  yielding a binary operation on  $\text{set\_End}(M)$  is defined by the term

(Def. 5)  $\text{FuncComp}(M) \upharpoonright (\text{set\_End}(M) \times \text{set\_End}(M))$ .

Now we state the proposition:

(6) Let us consider an Abelian group  $M$ , and endomorphisms  $f, g$  of  $M$ . Then

(i)  $f, g \in (\text{the carrier of } M)^\alpha$ , and

(ii)  $(\text{mult\_End}(M))(\langle f, g \rangle) = (\text{FuncComp}(M))(f, g)$ , and

(iii)  $(\text{FuncComp}(M))(f, g)$  is an endomorphism of  $M$ ,

where  $\alpha$  is the carrier of  $M$ . The theorem is a consequence of (5).

Let  $M$  be an Abelian group. The functors:  $0\_End(M)$  and  $1\_End(M)$  yielding elements of  $\text{set\_End}(M)$  are defined by terms

(Def. 6)  $\text{ZeroMap}(M, M)$ ,

(Def. 7)  $\text{id}_M$ ,

respectively. Let  $f$  be an element of  $\text{set\_End}(M)$ . The functor  $\text{Inv } f$  yielding an element of  $\text{set\_End}(M)$  is defined by

(Def. 8) for every element  $x$  of  $M$ ,  $it(x) = f(-x)$ .

Now we state the proposition:

(7) Let us consider an Abelian group  $M$ , and an element  $f$  of  $\text{set\_End}(M)$ . Then  $(\text{ADD}(M, M))(f, \text{Inv } f) = \text{ZeroMap}(M, M)$ .

PROOF: Consider  $f_1$  being a function from the carrier of  $M$  into the carrier of  $M$  such that  $f_1 = f$  and  $f_1$  is an endomorphism of  $M$ . Consider  $g_1$  being a function from the carrier of  $M$  into the carrier of  $M$  such that  $g_1 = \text{Inv } f$  and  $g_1$  is an endomorphism of  $M$ . For every element  $x$  of the carrier of  $M$ ,  $(\text{ADD}(M, M))(f_1, g_1)(x) = (\text{ZeroMap}(M, M))(x)$ .  $\square$

We define the Ring of Endomorphism of  $M$  as a structure.

Let  $M$  be an Abelian group. The functor  $\text{End\_Ring}(M)$  yielding a strict, non empty double loop structure is defined by the term

(Def. 9)  $\langle \text{set\_End}(M), \text{add\_End}(M), \text{mult\_End}(M), 1\_End(M), 0\_End(M) \rangle$ .

Now we state the proposition:

(8) THE STRUCTURE OF  $\text{END-RING}(M)$  TURNS TO BE A RING:

Let us consider an Abelian group  $M$ . Then  $\text{End\_Ring}(M)$  is a ring.

Let  $M$  be an Abelian group. One can verify that  $\text{End\_Ring}(M)$  is Abelian, add-associative, right zeroed, right complementable, associative, well unital, and distributive and  $\text{End\_Ring}(M)$  is strict.

In the sequel  $R$  denotes a ring and  $r$  denotes an element of  $R$ .

Let us consider  $R$ . Let  $M, N$  be left modules over  $R$ .

A homomorphism from  $M$  to  $N$  by  $R$  is a function from  $M$  into  $N$  defined by

(Def. 10) *it is additive and homogeneous.*

Now we state the proposition:

(9) Let us consider left modules  $M, N$  over  $R$ , and a homomorphism  $f$  from  $M$  to  $N$  by  $R$ . Suppose  $f$  is one-to-one and onto. Then  $f^{-1}$  is a homomorphism from  $N$  to  $M$  by  $R$ .

PROOF: Reconsider  $g = f^{-1}$  as a function from  $N$  into  $M$ . For every elements  $a, b$  of the carrier of  $N$ ,  $g(a+b) = g(a) + g(b)$ . For every element  $r$  of  $R$  and for every element  $a$  of the carrier of  $N$ ,  $g(r \cdot a) = r \cdot g(a)$ .  $\square$

Let us consider  $R$ . Let  $M, N$  be left modules over  $R$ . We say that  $M \cong N$  if and only if

(Def. 11) there exists a homomorphism  $f$  from  $M$  to  $N$  by  $R$  such that  $f$  is one-to-one and onto.

Let  $M$  be a left module over  $R$ .

An endomorphism of  $R$  and  $M$  is a homomorphism from  $M$  to  $M$  by  $R$ . Now we state the propositions:

(10) Let us consider a left module  $M$  over  $R$ . Then  $M \cong M$ .

(11) Let us consider left modules  $M, N$  over  $R$ . If  $M \cong N$ , then  $N \cong M$ .

The theorem is a consequence of (9).

Let us consider  $R$ . Let  $M, N$  be left modules over  $R$ . Observe that the predicate  $M \cong N$  is reflexive and symmetric. Now we state the propositions:

(12) Let us consider left modules  $L, M, N$  over  $R$ . If  $L \cong M$  and  $M \cong N$ , then  $L \cong N$ .

PROOF: Consider  $f$  being a homomorphism from  $L$  to  $M$  by  $R$  such that  $f$  is one-to-one and onto. Consider  $g$  being a homomorphism from  $M$  to  $N$  by  $R$  such that  $g$  is one-to-one and onto. Reconsider  $G = g \cdot f$  as a function from  $L$  into  $N$ . For every elements  $x, y$  of  $L$ ,  $G(x+y) = G(x) + G(y)$ . For every element  $x$  of  $L$  and for every element  $a$  of  $R$ ,  $G(a \cdot x) = a \cdot G(x)$ .  $\square$

(13) Let us consider left modules  $M, N$  over  $R$ , and a homomorphism  $f$  from  $M$  to  $N$  by  $R$ . Then  $f$  is one-to-one if and only if  $\ker f = \{0_M\}$ .

PROOF: If  $f$  is one-to-one, then  $\ker f = \{0_M\}$ . For every objects  $x_1, x_2$  such that  $x_1, x_2 \in \text{dom } f$  and  $f(x_1) = f(x_2)$  holds  $x_1 = x_2$ .  $\square$

Let us consider  $R$ . Let  $M$  be an Abelian group and  $s$  be a function from  $R$  into  $\text{End\_Ring}(M)$ . The functor  $\text{LModlmult}(M, s)$  yielding a function from (the carrier of  $R$ )  $\times$  (the carrier of  $M$ ) into the carrier of  $M$  is defined by

(Def. 12) for every element  $x$  of the carrier of  $R$  and for every element  $y$  of the carrier of  $M$ , there exists an endomorphism  $h$  of  $M$  such that  $h = s(x)$  and  $it(x, y) = h(y)$ .

The functor  $\text{AbGrLMod}(M, s)$  yielding a strict, non empty vector space structure over  $R$  is defined by the term

(Def. 13)  $\langle \text{the carrier of } M, \text{the addition of } M, 0_M, \text{LModlmult}(M, s) \rangle$ .

Now we state the proposition:

(14) Let us consider an Abelian group  $M$ , and a function  $s$  from  $R$  into  $\text{End\_Ring}(M)$ . Suppose  $s$  inherits ring homomorphism.

Then  $\text{AbGrLMod}(M, s)$  is a left module over  $R$ .

PROOF:  $\text{AbGrLMod}(M, s)$  is Abelian.  $\text{AbGrLMod}(M, s)$  is add-associative.  $\text{AbGrLMod}(M, s)$  is right zeroed.  $\text{AbGrLMod}(M, s)$  is right complementable.  $\text{AbGrLMod}(M, s)$  is scalar unital.  $\square$

The set of all functions from  $R$ -module  $M$  into  $R$ -module  $N$  form  $R$ -module. In the sequel  $M, N$  denote left modules over  $R$ .

Let us consider  $R, M$ , and  $N$ . The functor  $0\_Funcs(M, N)$  yielding an element of (the carrier of  $N$ )<sup>(the carrier of  $M$ )</sup> is defined by the term

(Def. 14)  $\text{ZeroMap}(M, N)$ .

The functor  $\text{ADD}(M, N)$  yielding a binary operation on (the carrier of  $N$ )<sup>(the carrier of  $M$ )</sup> is defined by

(Def. 15) for every elements  $f, g$  of (the carrier of  $N$ ) <sup>$\alpha$</sup> ,  $it(f, g) = (\text{the addition of } N)^\circ(f, g)$ , where  $\alpha$  is the carrier of  $M$ .

From now on  $f, g, h$  denote elements of (the carrier of  $N$ )<sup>(the carrier of  $M$ )</sup>.

Now we state the proposition:

(15)  $h = (\text{ADD}(M, N))(f, g)$  if and only if for every element  $x$  of the carrier of  $M$ ,  $h(x) = f(x) + g(x)$ .

Let us consider  $R, M$ , and  $N$ . Let  $F$  be a function from (the carrier of  $R$ )  $\times$  (the carrier of  $N$ ) into the carrier of  $N$ ,  $a$  be an element of the carrier of  $R$ , and  $f$  be a function from  $M$  into  $N$ . Observe that the functor  $F^\circ(a, f)$  yields an element of (the carrier of  $N$ )<sup>(the carrier of  $M$ )</sup>. The functor  $\text{LMULT}(M, N)$  yielding a function from (the carrier of  $R$ )  $\times$  (the carrier of  $N$ )<sup>(the carrier of  $M$ )</sup> into (the carrier of  $N$ )<sup>(the carrier of  $M$ )</sup> is defined by

(Def. 16) for every element  $a$  of the carrier of  $R$  and for every element  $f$  of (the carrier of  $N$ ) <sup>$\alpha$</sup>  and for every element  $x$  of the carrier of  $M$ ,  $it(\langle a, f \rangle)(x) = a \cdot f(x)$ , where  $\alpha$  is the carrier of  $M$ .

The functor  $\text{Func\_Mod}(R, M, N)$  yielding a non empty vector space structure over  $R$  is defined by the term

(Def. 17)  $\langle (\text{the carrier of } N)^\alpha, \text{ADD}(M, N), \mathbf{0\_Funcs}(M, N), \text{LMULT}(M, N) \rangle$ , where  $\alpha$  is the carrier of  $M$ .

Now we state the proposition:

(16) Let us consider an element  $a$  of the carrier of  $R$ , and elements  $f, h$  of  $(\text{the carrier of } N)^\alpha$ . Then  $h = (\text{LMULT}(M, N))(\langle a, f \rangle)$  if and only if for every element  $x$  of  $M$ ,  $h(x) = a \cdot f(x)$ , where  $\alpha$  is the carrier of  $M$ .

In the sequel  $a, b$  denote elements of the carrier of  $R$ .

Let us consider  $R, M$ , and  $N$ . Note that  $\text{Func\_Mod}(R, M, N)$  is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital. Now we state the proposition:

(17)  $\text{Func\_Mod}(R, M, N)$  is a left module over  $R$ .

From now on  $R$  denotes a commutative ring and  $M, M_1, N, N_1$  denote left modules over  $R$ . Now we state the proposition:

(18)  $\text{HOM}(M, N)$  THE SET OF ALL  $R$  HOMOMORPHISMS FORM LEFT  $R$ -MODULE:

Let us consider homomorphisms  $f, g$  from  $M$  to  $N$  by  $R$ .

Then  $(\text{ADD}(M, N))(f, g)$  is a homomorphism from  $M$  to  $N$  by  $R$ . The theorem is a consequence of (15).

Let us consider  $R, M_1, M$ , and  $N$ . Let  $f$  be an element of  $(\text{the carrier of } M)^{(\text{the carrier of } M_1)}$  and  $g$  be an element of  $(\text{the carrier of } N)^{(\text{the carrier of } M)}$ . Let us observe that the functor  $g \cdot f$  yields an element of  $(\text{the carrier of } N)^{(\text{the carrier of } M_1)}$ . Now we state the propositions:

(19) Let us consider left modules  $M, N, M_1$  over  $R$ , a homomorphism  $f$  from  $M$  to  $N$  by  $R$ , and a homomorphism  $u$  from  $M_1$  to  $M$  by  $R$ . Then  $f \cdot u$  is a homomorphism from  $M_1$  to  $N$  by  $R$ .

PROOF: For every elements  $x_1, y_1$  of the carrier of  $M_1$  and for every element  $a$  of  $R$ ,  $(f \cdot u)(x_1 + y_1) = (f \cdot u)(x_1) + (f \cdot u)(y_1)$  and  $a \cdot (f \cdot u)(x_1) = a \cdot (f \cdot u)(x_1)$ . For every element  $x_1$  of the carrier of  $M_1$  and for every element  $a$  of  $R$ ,  $(f \cdot u)(a \cdot x_1) = a \cdot (f \cdot u)(x_1)$ .  $\square$

(20) Let us consider an element  $a$  of the carrier of  $R$ , and a homomorphism  $g$  from  $M$  to  $N$  by  $R$ . Then  $(\text{LMULT}(M, N))(\langle a, g \rangle)$  is a homomorphism from  $M$  to  $N$  by  $R$ .

Let us consider  $R, M$ , and  $N$ . The functor  $\text{set\_Hom}(M, N)$  yielding a non empty subset of  $(\text{the carrier of } N)^{(\text{the carrier of } M)}$  is defined by the term

(Def. 18)  $\{f, \text{ where } f \text{ is a function from } M \text{ into } N : f \text{ is a homomorphism from } M \text{ to } N \text{ by } R\}$ .

The functor  $\text{add\_Hom}(M, N)$  yielding a binary operation on  $\text{set\_Hom}(M, N)$  is defined by the term

(Def. 19)  $\text{ADD}(M, N) \upharpoonright (\text{set\_Hom}(M, N) \times \text{set\_Hom}(M, N))$ .

Let  $F$  be a function from  $(\text{the carrier of } R) \times (\text{the carrier of } N)$  into the carrier of  $N$ ,  $a$  be an element of the carrier of  $R$ , and  $f$  be a function from  $M$  into  $N$ . One can verify that the functor  $F^\circ(a, f)$  yields an element of  $(\text{the carrier of } N)^{(\text{the carrier of } M)}$ . The functor  $\text{lmult\_Hom}(M, N)$  yielding a function from  $(\text{the carrier of } R) \times \text{set\_Hom}(M, N)$  into  $\text{set\_Hom}(M, N)$  is defined by the term

(Def. 20)  $\text{LMULT}(M, N) \upharpoonright ((\text{the carrier of } R) \times \text{set\_Hom}(M, N))$ .

The functor  $0\_Hom(M, N)$  yielding an element of  $\text{set\_Hom}(M, N)$  is defined by the term

(Def. 21)  $\text{ZeroMap}(M, N)$ .

The functor  $\text{Hom}(R, M, N)$  yielding a non empty vector space structure over  $R$  is defined by the term

(Def. 22)  $\langle \text{set\_Hom}(M, N), \text{add\_Hom}(M, N), 0\_Hom(M, N), \text{lmult\_Hom}(M, N) \rangle$ .

Let us note that  $\text{Hom}(R, M, N)$  is non empty. Now we state the propositions:

(21) Let us consider homomorphisms  $f, g$  from  $M$  to  $N$  by  $R$ . Then

(i)  $f, g \in (\text{the carrier of } N)^\alpha$ , and

(ii)  $(\text{add\_Hom}(M, N))(\langle f, g \rangle) = (\text{ADD}(M, N))(f, g)$ , and

(iii)  $(\text{ADD}(M, N))(f, g)$  is a homomorphism from  $M$  to  $N$  by  $R$ ,

where  $\alpha$  is the carrier of  $M$ . The theorem is a consequence of (18).

(22) Let us consider an element  $a$  of the carrier of  $R$ , and a homomorphism  $f$  from  $M$  to  $N$  by  $R$ . Then

(i)  $(\text{lmult\_Hom}(M, N))(\langle a, f \rangle) = (\text{LMULT}(M, N))(\langle a, f \rangle)$ , and

(ii)  $(\text{LMULT}(M, N))(\langle a, f \rangle)$  is a homomorphism from  $M$  to  $N$  by  $R$ .

The theorem is a consequence of (20).

(23) Let us consider elements  $f_1, g_1$  of  $\text{Func\_Mod}(R, M, N)$ , and elements  $f, g$  of  $\text{Hom}(R, M, N)$ . If  $f_1 = f$  and  $g_1 = g$ , then  $f + g = f_1 + g_1$ . The theorem is a consequence of (21).

(24)  $\text{Hom}(R, M, N)$  is a left module over  $R$ . The theorem is a consequence of (23).

Let us consider  $R, M$ , and  $N$ . Note that  $\text{Hom}(R, M, N)$  is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

Let us consider  $M_1$ . Let  $u$  be a homomorphism from  $M_1$  to  $M$  by  $R$ . The functor  $\tau(N, u)$  yielding a function from  $\text{Hom}(R, M, N)$  into  $\text{Hom}(R, M_1, N)$  is defined by

(Def. 23) for every element  $f$  of  $\text{Hom}(R, M, N)$ , there exists a homomorphism  $f_1$  from  $M$  to  $N$  by  $R$  such that  $f = f_1$  and  $it(f) = f_1 \cdot u$ .

Let us note that  $\tau(N, u)$  is additive and homogeneous. Now we state the proposition:

(25) Let us consider a homomorphism  $u$  from  $M_1$  to  $M$  by  $R$ . Then  $\tau(N, u)$  is a homomorphism from  $\text{Hom}(R, M, N)$  to  $\text{Hom}(R, M_1, N)$  by  $R$ .

Let us consider  $R, M, N$ , and  $N_1$ . Let  $u$  be a homomorphism from  $N$  to  $N_1$  by  $R$ . The functor  $\phi(M, u)$  yielding a function from  $\text{Hom}(R, M, N)$  into  $\text{Hom}(R, M, N_1)$  is defined by

(Def. 24) for every element  $f$  of  $\text{Hom}(R, M, N)$ , there exists a homomorphism  $f_1$  from  $M$  to  $N$  by  $R$  such that  $f = f_1$  and  $it(f) = u \cdot f_1$ .

Let us observe that  $\phi(M, u)$  is additive and homogeneous. Now we state the propositions:

(26) Let us consider a homomorphism  $u$  from  $N$  to  $N_1$  by  $R$ . Then  $\phi(M, u)$  is a homomorphism from  $\text{Hom}(R, M, N)$  to  $\text{Hom}(R, M, N_1)$  by  $R$ .

(27)  $\text{Hom}(R, \text{LeftMod}(R), M) \cong M$ .

PROOF: Reconsider  $R_1 = \text{LeftMod}(R)$  as a left module over  $R$ . Reconsider  $m_1 = 1_R$  as an element of  $R_1$ . Define  $\mathcal{F}$ (element of (the carrier of  $M$ )(the carrier of  $R_1$ )) =  $\$1(m_1)$ . Consider  $G$  being a function from (the carrier of  $M$ )(the carrier of  $R_1$ ) into  $M$  such that For every element  $x$  of (the carrier of  $M$ ) $^\alpha$ ,  $G(x) = \mathcal{F}(x)$ , where  $\alpha$  is the carrier of  $R_1$ . For every elements  $f, g$  of (the carrier of  $M$ ) $^\alpha$ ,  $G((\text{ADD}(R_1, M))(f, g)) = G(f) + G(g)$ , where  $\alpha$  is the carrier of  $R_1$ .

For every element  $f$  of (the carrier of  $M$ ) $^\alpha$  and for every element  $a$  of  $R$ ,  $G((\text{LMULT}(R_1, M))(\langle a, f \rangle)) = a \cdot G(f)$ , where  $\alpha$  is the carrier of  $R_1$ . Set  $c =$  the carrier of  $\text{Hom}(R, R_1, M)$ . Set  $G_1 = G|_c$ . For every object  $y$  such that  $y \in \text{rng } G_1$  holds  $y \in$  the carrier of  $M$ . For every elements  $f, g$  of  $\text{Hom}(R, R_1, M)$ ,  $G_1(f + g) = G_1(f) + G_1(g)$ . For every element  $f$  of  $\text{Hom}(R, R_1, M)$  and for every element  $a$  of  $R$ ,  $G_1(a \cdot f) = a \cdot G_1(f)$ .  $\ker G_1 = \{0_{\text{Hom}(R, R_1, M)}\}$ . For every object  $y$  such that  $y \in$  the carrier of  $M$  holds  $y \in \text{rng } G_1$ .  $\square$

Correspondence between Abelian Group (AbGr) and left  $R$ -module.

Let us consider  $R$  and  $M$ . The functor  $\text{AbGr}(M)$  yielding a non empty, strict Abelian group is defined by the term

(Def. 25)  $\langle \text{the carrier of } M, \text{the addition of } M, 0_M \rangle$ .

Let us consider  $N$ . Let  $f$  be a homomorphism from  $M$  to  $N$  by  $R$ . The functor  $\text{AbGr}(f)$  yielding a function from  $\text{AbGr}(M)$  into  $\text{AbGr}(N)$  is defined by



(Def. 26) for every object  $x$  such that  $x \in$  the carrier of  $\text{AbGr}(M)$  holds  $it(x) = f(x)$ .

Now we state the proposition:

(28) Let us consider a homomorphism  $f$  from  $M$  to  $N$  by  $R$ . Then  $\text{AbGr}(f)$  is a homomorphism from  $\text{AbGr}(M)$  to  $\text{AbGr}(N)$ .

Let us consider endomorphisms  $f, g, h$  of  $R$  and  $M$ . Now we state the propositions:

(29)  $\text{AbGr}(h) = (\text{FuncComp}(\text{AbGr}(M)))(\text{AbGr}(f), \text{AbGr}(g))$  if and only if for every element  $x$  of the carrier of  $\text{AbGr}(M)$ ,  $(\text{AbGr}(h))(x) = ((\text{AbGr}(f)) \cdot (\text{AbGr}(g)))(x)$ .

(30) If  $h = f \cdot g$ , then  $\text{AbGr}(h) = (\text{AbGr}(f)) \cdot (\text{AbGr}(g))$ .

PROOF: For every element  $x$  of the carrier of  $\text{AbGr}(M)$ ,  $(\text{AbGr}(h))(x) = ((\text{AbGr}(f)) \cdot (\text{AbGr}(g)))(x)$ .  $\square$

(31)  $\text{AbGr}(h) = (\text{ADD}(\text{AbGr}(M), \text{AbGr}(M)))(\text{AbGr}(f), \text{AbGr}(g))$  if and only if for every element  $x$  of the carrier of  $\text{AbGr}(M)$ ,  $(\text{AbGr}(h))(x) = (\text{AbGr}(f))(x) + (\text{AbGr}(g))(x)$ .

PROOF: If  $\text{AbGr}(h) = (\text{ADD}(\text{AbGr}(M), \text{AbGr}(M)))(\text{AbGr}(f), \text{AbGr}(g))$ , then for every element  $x$  of the carrier of  $\text{AbGr}(M)$ ,  $(\text{AbGr}(h))(x) = (\text{AbGr}(f))(x) + (\text{AbGr}(g))(x)$ .  $\text{AbGr}(h) = (\text{ADD}(\text{AbGr}(M), \text{AbGr}(M)))(\text{AbGr}(f), \text{AbGr}(g))$ .  $\square$

(32) If  $h = (\text{ADD}(M, M))(f, g)$ , then  $\text{AbGr}(h) = (\text{ADD}(\text{AbGr}(M), \text{AbGr}(M)))(\text{AbGr}(f), \text{AbGr}(g))$ . The theorem is a consequence of (15) and (31).

(33) Let us consider a ring  $R$ , a left module  $M$  over  $R$ , an element  $a$  of  $R$ , and an element  $m$  of  $M$ . Then  $(\text{curry}(\text{the left multiplication of } M))(a)(m) = a \cdot m$ .

(34) Let us consider a commutative ring  $R$ , a left module  $M$  over  $R$ , and an element  $a$  of  $R$ . Then  $(\text{curry}(\text{the left multiplication of } M))(a)$  is an endomorphism of  $R$  and  $M$ .

PROOF: Set  $f = (\text{curry}(\text{the left multiplication of } M))(a)$ . For every elements  $m_1, m_2$  of  $M$ ,  $f(m_1 + m_2) = f(m_1) + f(m_2)$ . For every element  $b$  of  $R$  and for every element  $m$  of  $M$ ,  $f(b \cdot m) = b \cdot f(m)$ .  $\square$

(35) Let us consider endomorphisms  $f, g, h$  of  $R$  and  $M$ . Suppose  $h = f \cdot g$ . Then  $\text{AbGr}(h) = (\text{FuncComp}(\text{AbGr}(M)))(\text{AbGr}(f), \text{AbGr}(g))$ . The theorem is a consequence of (30) and (29).

Let  $R$  be a commutative ring and  $M$  be a left module over  $R$ . The canonical homomorphism of  $M$  into quotient field yielding a function from  $R$  into  $\text{End\_Ring}(\text{AbGr}(M))$  is defined by

(Def. 27) for every object  $x$  such that  $x \in$  the carrier of  $R$  there exists an endomorphism  $f$  of  $R$  and  $M$  such that  $f = (\text{curry}(\text{the left multiplication of } M))(x)$  and  $it(x) = \text{AbGr}(f)$ .

Observe that the canonical homomorphism of  $M$  into quotient field is additive. Now we state the proposition:

(36) Let us consider a commutative ring  $R$ , a left module  $M$  over  $R$ , and an element  $a$  of  $R$ . Then (the canonical homomorphism of  $M$  into quotient field)( $a$ ) is a homomorphism from  $\text{AbGr}(M)$  to  $\text{AbGr}(M)$ .

Let  $R$  be a commutative ring and  $M$  be a left module over  $R$ . One can verify that the canonical homomorphism of  $M$  into quotient field is linear and  $\text{AbGrLMod}(\text{AbGr}(M))$ , the canonical homomorphism of  $M$  into quotient field) is non empty, Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

Now we state the propositions:

(37) Let us consider a commutative ring  $R$ , and a left module  $M$  over  $R$ . Then  $\text{LModmult}(\text{AbGr}(M))$ , the canonical homomorphism of  $M$  into quotient field) = the left multiplication of  $M$ .

PROOF: Set  $F = \text{LModmult}(\text{AbGr}(M))$ , the canonical homomorphism of  $M$  into quotient field). For every object  $z$  such that  $z \in$  (the carrier of  $R$ )  $\times$  (the carrier of  $M$ ) holds  $F(z) =$  (the left multiplication of  $M$ )( $z$ ).  $\square$

(38) Let us consider a commutative ring  $R$ , and a strict left module  $M$  over  $R$ . Then  $\text{AbGrLMod}(\text{AbGr}(M))$ , the canonical homomorphism of  $M$  into quotient field) =  $M$ .

PROOF:  $\text{AbGrLMod}(\text{AbGr}(M))$ , the canonical homomorphism of  $M$  into quotient field) is a submodule of  $M$ .  $\square$

Let  $R$  be a commutative ring and  $M$  be a left module over  $R$ . The functor  $\rho(M)$  yielding a function from  $M$  into  $\text{AbGrLMod}(\text{AbGr}(M))$ , the canonical homomorphism of  $M$  into quotient field) is defined by the term

(Def. 28)  $\text{id}_M$ .

Now we state the proposition:

(39) Let us consider a commutative ring  $R$ , and a left module  $M$  over  $R$ . Then  $\rho(M)$  is additive and homogeneous.

PROOF: For every element  $x$  of the carrier of  $M$  and for every element  $a$  of  $R$ ,  $\rho(M)(a \cdot x) = a \cdot \rho(M)(x)$  by [5, (7)].  $\square$

Let  $R$  be a commutative ring and  $M$  be a left module over  $R$ . Observe that  $\rho(M)$  is additive and homogeneous.

Let us consider a commutative ring  $R$  and a left module  $M$  over  $R$ . Now we state the propositions:

- (40)  $\rho(M)$  is one-to-one and onto.
- (41)  $M \cong \text{AbGrLMod}(\text{AbGr}(M))$ , the canonical homomorphism of  $M$  into quotient field). The theorem is a consequence of (40).

## REFERENCES

- [1] Frank W. Anderson and Kent R. Fuller. *Rings and Categories of Modules, Second Edition*. Springer-Verlag, 1992.
- [2] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*, volume 2. Addison-Wesley Reading, 1969.
- [3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8\_17.
- [4] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.
- [5] Kazuhisa Nakasho, Yuichi Futa, and Yasunari Shidama. Continuity of bounded linear operators on normed linear spaces. *Formalized Mathematics*, 26(3):231–237, 2018. doi:10.2478/forma-2018-0021.

*Accepted September 30, 2022*

---