FORMALIZED MATHEMATICS
Vol.2, No.1, January–February 1991
Université Catholique de Louvain

Construction of Rings and Left-, Right-, and Bi-Modules over a Ring

Michał Muzalewski[1]
Warsaw University
Białystok

Summary. Definitions of some classes of rings and left-, right-, and bi-modules over a ring and some elementary theorems on rings and skew fields.

MML Identifier: `VECTSP_2`.

The articles [9], [8], [11], [3], [1], [10], [7], [4], [2], [5], and [6] provide the notation and terminology for this paper. In the sequel F_1 will denote a field structure. Let us consider F_1. A scalar of F_1 is an element of the carrier of F_1.

In the sequel x, y will denote scalars of F_1. Let us consider F_1, x, y. The functor $x - y$ yields a scalar of F_1 and is defined as follows:

(Def.1) $x - y = x + (-y)$.

In the sequel F denotes a field. A field structure is called a ring if:

(Def.2) Let x, y, z be scalars of it . Then

- (i) $x + y = y + x$,
- (ii) $(x + y) + z = x + (y + z)$,
- (iii) $x + 0_{\rm it} = x$,
- (iv) $x + (-x) = 0_{\rm it}$,
- (v) $x \cdot (1_{\rm it}) = x$,
- (vi) $(1_{\rm it}) \cdot x = x$,
- (vii) $x \cdot (y + z) = x \cdot y + x \cdot z$,
- (viii) $(y + z) \cdot x = y \cdot x + z \cdot x$.

The following proposition is true

[1]Supported by RPBP.III-24.C6.

ISSN 0777–4028

(1) The following conditions are equivalent:

(i) for all scalars x, y, z of F_1 holds $x+y = y+x$ and $(x+y)+z = x+(y+z)$ and $x + 0_{F_1} = x$ and $x + (-x) = 0_{F_1}$ and $x \cdot (1_{F_1}) = x$ and $(1_{F_1}) \cdot x = x$ and $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$,

(ii) F_1 is a ring.

In the sequel R is a ring and x, y, z are scalars of R. Next we state several propositions:

(2) $x + y = y + x$.

(3) $(x + y) + z = x + (y + z)$.

(4) $x + 0_R = x$.

(5) $x + (-x) = 0_R$.

(6) $x \cdot (1_R) = x$ and $(1_R) \cdot x = x$.

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

A ring is called an associative ring if:

(Def.3) for all scalars x, y, z of it holds $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

The following proposition is true

(8) For all scalars x, y, z of R holds $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ if and only if R is an associative ring.

In the sequel R will denote an associative ring and x, y, z will denote scalars of R. One can prove the following proposition

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

An associative ring is said to be a commutative ring if:

(Def.4) for all scalars x, y of it holds $x \cdot y = y \cdot x$.

One can prove the following proposition

(10) If for all scalars x, y of R holds $x \cdot y = y \cdot x$, then R is a commutative ring.

In the sequel R will denote a commutative ring and x, y will denote scalars of R. The following proposition is true

(11) $x \cdot y = y \cdot x$.

A commutative ring is said to be an integral domain if:

(Def.5) $0_{\rm it} \neq 1_{\rm it}$ and for all scalars x, y of it such that $x \cdot y = 0_{\rm it}$ holds $x = 0_{\rm it}$ or $y = 0_{\rm it}$.

We now state two propositions:

(12) If $0_R \neq 1_R$ and for all x, y such that $x \cdot y = 0_R$ holds $x = 0_R$ or $y = 0_R$, then R is an integral domain.

(13) F is an integral domain.

In the sequel R denotes an integral domain and x, y denote scalars of R. The following propositions are true:

(14) $0_R \neq 1_R$.

(15) If $x \cdot y = 0_R$, then $x = 0_R$ or $y = 0_R$.

An associative ring is called a skew field if:

(Def.6) for every scalar x of it holds if $x \neq 0_{\rm it}$, then there exists a scalar y of it such that $x \cdot y = 1_{\rm it}$ but $0_{\rm it} \neq 1_{\rm it}$.

In the sequel R denotes an associative ring. The following proposition is true

(16) If for every scalar x of R holds if $x \neq 0_R$, then there exists a scalar y of R such that $x \cdot y = 1_R$ but $0_R \neq 1_R$, then R is a skew field.

In the sequel S_1 will denote a skew field and x, y will denote scalars of S_1. The following propositions are true:

(17) If $x \neq 0_{S_1}$, then there exists y such that $x \cdot y = 1_{S_1}$.

(18) $0_{S_1} \neq 1_{S_1}$.

(19) F is a skew field.

We see that the field is a skew field.

In the sequel R is a ring and x, y, z are scalars of R. Next we state a number of propositions:

(20) $x - y = x + (-y)$.

(21) $-0_R = 0_R$.

(22) $x + y = z$ if and only if $x = z - y$ but $x + y = z$ if and only if $y = z - x$.

(23) $x - 0_R = x$ and $0_R - x = -x$.

(24) If $x + y = x + z$, then $y = z$ but if $x + y = z + y$, then $x = z$.

(25) $-(x + y) = (-x) + (-y)$.

(26) $x \cdot 0_R = 0_R$ and $0_R \cdot x = 0_R$.

(27) $-(-x) = x$.

(28) $(-x) \cdot y = -x \cdot y$.

(29) $x \cdot (-y) = -x \cdot y$.

(30) $(-x) \cdot (-y) = x \cdot y$.

(31) $x \cdot (y - z) = x \cdot y - x \cdot z$.

(32) $(x - y) \cdot z = x \cdot z - y \cdot z$.

(33) $(x + y) - z = x + (y - z)$.

(34) $x = 0_R$ if and only if $-x = 0_R$.

(35) $x - (y + z) = (x - y) - z$.

(36) $x - (y - z) = (x - y) + z$.

(37) $x - x = 0_R$ and $(-x) + x = 0_R$.

(38) For every x, y there exists z such that $x = y + z$ and $x = z + y$.

In the sequel S_1 denotes a skew field and x, y, z denote scalars of S_1. We now state four propositions:

(39) If $x \cdot y = 1_{S_1}$, then $x \neq 0_{S_1}$ and $y \neq 0_{S_1}$.

(40) If $x \neq 0_{S_1}$, then there exists y such that $y \cdot x = 1_{S_1}$.

(41) If $x \cdot y = 1_{S_1}$, then $y \cdot x = 1_{S_1}$.

(42) If $x \cdot y = x \cdot z$ and $x \neq 0_{S_1}$, then $y = z$.

Let us consider S_1, x. Let us assume that $x \neq 0_{S_1}$. The functor x^{-1} yielding a scalar of S_1 is defined by:

(Def.7) $x \cdot (x^{-1}) = 1_{S_1}$.

Let us consider S_1, x, y. Let us assume that $y \neq 0_{S_1}$. The functor $\frac{x}{y}$ yielding a scalar of S_1 is defined by:

(Def.8) $\frac{x}{y} = x \cdot y^{-1}$.

One can prove the following propositions:

(43) If $x \neq 0_{S_1}$, then $x \cdot x^{-1} = 1_{S_1}$ and $x^{-1} \cdot x = 1_{S_1}$.

(44) If $y \neq 0_{S_1}$, then $\frac{x}{y} = x \cdot y^{-1}$.

(45) If $x \cdot y = 1_{S_1}$, then $x = y^{-1}$ and $y = x^{-1}$.

(46) If $x \neq 0_{S_1}$ and $y \neq 0_{S_1}$, then $x^{-1} \cdot y^{-1} = (y \cdot x)^{-1}$.

(47) If $x \cdot y = 0_{S_1}$, then $x = 0_{S_1}$ or $y = 0_{S_1}$.

(48) If $x \neq 0_{S_1}$, then $x^{-1} \neq 0_{S_1}$.

(49) If $x \neq 0_{S_1}$, then $(x^{-1})^{-1} = x$.

(50) If $x \neq 0_{S_1}$, then $\frac{1_{S_1}}{x} = x^{-1}$ and $\frac{1_{S_1}}{x^{-1}} = x$.

(51) If $x \neq 0_{S_1}$, then $x \cdot \frac{1_{S_1}}{x} = 1_{S_1}$ and $\frac{1_{S_1}}{x} \cdot x = 1_{S_1}$.

(52) If $x \neq 0_{S_1}$, then $\frac{x}{x} = 1_{S_1}$.

(53) If $y \neq 0_{S_1}$ and $z \neq 0_{S_1}$, then $\frac{x}{y} = \frac{x \cdot z}{y \cdot z}$.

(54) If $y \neq 0_{S_1}$, then $-\frac{x}{y} = \frac{-x}{y}$ and $\frac{x}{-y} = -\frac{x}{y}$.

(55) If $z \neq 0_{S_1}$, then $\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z}$ and $\frac{x}{z} - \frac{y}{z} = \frac{x-y}{z}$.

(56) If $y \neq 0_{S_1}$ and $z \neq 0_{S_1}$, then $\frac{x}{\frac{y}{z}} = \frac{x \cdot z}{y}$.

(57) If $y \neq 0_{S_1}$, then $\frac{x}{y} \cdot y = x$.

Let us consider F_1. We consider left module structures over F_1 which are systems

$\langle$a carrier, a left multiplication$\rangle$,

where the carrier is an Abelian group and the left multiplication is a function from $[\!:$ the carrier of F_1, the carrier of the carrier $:\!]$ into the carrier of the carrier.

In the sequel L_1 denotes a left module structure over F_1. We now define two new modes. Let us consider F_1, L_1. A scalar of L_1 is a scalar of F_1.

A vector of L_1 is an element of the carrier of L_1.

Let us consider F_1. We consider right module structures over F_1 which are systems

$\langle$a carrier, a right multiplication$\rangle$,

where the carrier is an Abelian group and the right multiplication is a function from $[\!:$ the carrier of the carrier, the carrier of F_1 $:\!]$ into the carrier of the carrier.

In the sequel R_1 will denote a right module structure over F_1. We now define two new modes. Let us consider F_1, R_1. A scalar of R_1 is a scalar of F_1.

A vector of R_1 is an element of the carrier of R_1.

Let us consider F_1. We consider bimodule structures over F_1 which are systems

⟨a carrier, a left multiplication, a right multiplication⟩,

where the carrier is an Abelian group, the left multiplication is a function from $[\!:$ the carrier of F_1, the carrier of the carrier $:\!]$ into the carrier of the carrier, and the right multiplication is a function from $[\!:$ the carrier of the carrier, the carrier of F_1 $:\!]$ into the carrier of the carrier.

In the sequel B_1 will denote a bimodule structure over F_1. We now define two new modes. Let us consider F_1, B_1. A scalar of B_1 is a scalar of F_1.

A vector of B_1 is an element of the carrier of B_1.

In the sequel R is a ring. Let us consider R. The functor $\mathrm{AbGr}(R)$ yields an Abelian group and is defined by:

(Def.9) $\mathrm{AbGr}(R) = \langle$ the carrier of R, the addition of R, the reverse-map of R, the zero of $R\rangle$.

Next we state the proposition

(58) $\mathrm{AbGr}(R) = \langle$ the carrier of R, the addition of R, the reverse-map of R, the zero of $R\rangle$.

Let us consider R. The functor $\mathrm{LeftModMult}(R)$ yielding a function from $[\!:$ the carrier of R, the carrier of $\mathrm{AbGr}(R)$ $:\!]$ into the carrier of $\mathrm{AbGr}(R)$ is defined as follows:

(Def.10) $\mathrm{LeftModMult}(R) =$ the multiplication of R.

Next we state the proposition

(59) $\mathrm{LeftModMult}(R) =$ the multiplication of R.

Let us consider R. The functor $\mathrm{LeftMod}(R)$ yielding a left module structure over R is defined as follows:

(Def.11) $\mathrm{LeftMod}(R) = \langle \mathrm{AbGr}(R), \mathrm{LeftModMult}(R)\rangle$.

We now state the proposition

(60) $\mathrm{LeftMod}(R) = \langle \mathrm{AbGr}(R), \mathrm{LeftModMult}(R)\rangle$.

In the sequel V will be a left module structure over R. Let us consider R, V, and let x be a scalar of R, and let v be a vector of V. The functor $x \cdot v$ yielding a vector of V is defined as follows:

(Def.12) for every scalar x' of V such that $x' = x$ holds $x \cdot v =$ (the left multiplication of $V)(x', v)$.

The following proposition is true

(62)[2] For every V being a left module structure over R and for every scalar x of R and for every vector v of V and for every scalar x' of V such that $x' = x$ holds $x \cdot v =$ (the left multiplication of $V)(x', v)$.

Let us consider R. The functor $\mathrm{RightModMult}(R)$ yields a function from $[\!:$ the carrier of $\mathrm{AbGr}(R)$, the carrier of R $:\!]$ into the carrier of $\mathrm{AbGr}(R)$ and is defined as follows:

[2]The proposition (61) was either repeated or obvious.

(Def.13) RightModMult(R) = the multiplication of R.

We now state the proposition

(63) RightModMult(R) = the multiplication of R.

Let us consider R. The functor RightMod(R) yielding a right module structure over R is defined as follows:

(Def.14) $\mathrm{RightMod}(R) = \langle \mathrm{AbGr}(R), \mathrm{RightModMult}(R) \rangle$.

We now state the proposition

(64) $\mathrm{RightMod}(R) = \langle \mathrm{AbGr}(R), \mathrm{RightModMult}(R) \rangle$.

In the sequel V will denote a right module structure over R. Let us consider R, V, and let x be a scalar of R, and let v be a vector of V. The functor $v \cdot x$ yielding a vector of V is defined as follows:

(Def.15) for every scalar x' of V such that $x' = x$ holds $v \cdot x =$ (the right multiplication of V)(v, x').

We now state the proposition

(66)[3] For every V being a right module structure over R and for every scalar x of R and for every vector v of V and for every scalar x' of V such that $x' = x$ holds $v \cdot x =$ (the right multiplication of V)(v, x').

Let us consider R. The functor BiMod(R) yielding a bimodule structure over R is defined as follows:

(Def.16) $\mathrm{BiMod}(R) = \langle \mathrm{AbGr}(R), \mathrm{LeftModMult}(R), \mathrm{RightModMult}(R) \rangle$.

The following proposition is true

(67) $\mathrm{BiMod}(R) = \langle \mathrm{AbGr}(R), \mathrm{LeftModMult}(R), \mathrm{RightModMult}(R) \rangle$.

In the sequel V is a bimodule structure over R. Let us consider R, V, and let x be a scalar of R, and let v be a vector of V. The functor $x \cdot v$ yields a vector of V and is defined as follows:

(Def.17) for every scalar x' of V such that $x' = x$ holds $x \cdot v =$ (the left multiplication of V)(x', v).

One can prove the following proposition

(69)[4] For every V being a bimodule structure over R and for every scalar x of R and for every vector v of V and for every scalar x' of V such that $x' = x$ holds $x \cdot v =$ (the left multiplication of V)(x', v).

Let us consider R, V, and let x be a scalar of R, and let v be a vector of V. The functor $v \cdot x$ yields a vector of V and is defined by:

(Def.18) for every scalar x' of V such that $x' = x$ holds $v \cdot x =$ (the right multiplication of V)(v, x').

The following proposition is true

[3] The proposition (65) was either repeated or obvious.

[4] The proposition (68) was either repeated or obvious.

(70) For every V being a bimodule structure over R and for every scalar x of R and for every vector v of V and for every scalar x' of V such that $x' = x$ holds $v \cdot x =$ (the right multiplication of V)(v, x').

In the sequel R will denote an associative ring. Next we state the proposition

(71) Let x, y be scalars of R. Let v, w be vectors of LeftMod(R). Then $x \cdot (v+w) = x \cdot v + x \cdot w$ and $(x+y) \cdot v = x \cdot v + y \cdot v$ and $(x \cdot y) \cdot v = x \cdot (y \cdot v)$ and $(1_R) \cdot v = v$.

Let us consider R. A left module structure over R is called a left module over R if:

(Def.19) Let x, y be scalars of R. Let v, w be vectors of it . Then $x \cdot (v + w) = x \cdot v + x \cdot w$ and $(x + y) \cdot v = x \cdot v + y \cdot v$ and $(x \cdot y) \cdot v = x \cdot (y \cdot v)$ and $(1_R) \cdot v = v$.

We now state the proposition

(72) Let V be a left module structure over R. Then the following conditions are equivalent:

(i) for all scalars x, y of R and for all vectors v, w of V holds $x \cdot (v+w) = x \cdot v + x \cdot w$ and $(x + y) \cdot v = x \cdot v + y \cdot v$ and $(x \cdot y) \cdot v = x \cdot (y \cdot v)$ and $(1_R) \cdot v = v$,

(ii) V is a left module over R.

Let us consider R. Then LeftMod(R) is a left module over R.

For simplicity we adopt the following rules: R is an associative ring, x, y are scalars of R, L_2 is a left module over R, and v, w are vectors of L_2. We now state several propositions:

(73) $x \cdot (v + w) = x \cdot v + x \cdot w$.

(74) $(x + y) \cdot v = x \cdot v + y \cdot v$.

(75) $(x \cdot y) \cdot v = x \cdot (y \cdot v)$.

(76) $(1_R) \cdot v = v$.

(77) Let x, y be scalars of R. Let v, w be vectors of RightMod(R). Then $(v+w) \cdot x = v \cdot x + w \cdot x$ and $v \cdot (x+y) = v \cdot x + v \cdot y$ and $v \cdot (y \cdot x) = (v \cdot y) \cdot x$ and $v \cdot (1_R) = v$.

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

(Def.20) Let x, y be scalars of R. Let v, w be vectors of it . Then $(v + w) \cdot x = v \cdot x + w \cdot x$ and $v \cdot (x + y) = v \cdot x + v \cdot y$ and $v \cdot (y \cdot x) = (v \cdot y) \cdot x$ and $v \cdot (1_R) = v$.

The following proposition is true

(78) Let V be a right module structure over R. Then the following conditions are equivalent:

(i) for all scalars x, y of R and for all vectors v, w of V holds $(v+w) \cdot x = v \cdot x + w \cdot x$ and $v \cdot (x + y) = v \cdot x + v \cdot y$ and $v \cdot (y \cdot x) = (v \cdot y) \cdot x$ and $v \cdot (1_R) = v$,

(ii) V is a right module over R.

Let us consider R. Then RightMod(R) is a right module over R.

For simplicity we follow the rules: R is an associative ring, x, y are scalars of R, R_2 is a right module over R, and v, w are vectors of R_2. We now state four propositions:

(79) $(v + w) \cdot x = v \cdot x + w \cdot x$.

(80) $v \cdot (x + y) = v \cdot x + v \cdot y$.

(81) $v \cdot (y \cdot x) = (v \cdot y) \cdot x$.

(82) $v \cdot (1_R) = v$.

Let us consider R. A bimodule structure over R is said to be a bimodule over R if:

(Def.21) Let x, y be scalars of R. Let v, w be vectors of it . Then

(i) $x \cdot (v + w) = x \cdot v + x \cdot w$,
(ii) $(x + y) \cdot v = x \cdot v + y \cdot v$,
(iii) $(x \cdot y) \cdot v = x \cdot (y \cdot v)$,
(iv) $(1_R) \cdot v = v$,
(v) $(v + w) \cdot x = v \cdot x + w \cdot x$,
(vi) $v \cdot (x + y) = v \cdot x + v \cdot y$,
(vii) $v \cdot (y \cdot x) = (v \cdot y) \cdot x$,
(viii) $v \cdot (1_R) = v$,
(ix) $x \cdot (v \cdot y) = (x \cdot v) \cdot y$.

Next we state two propositions:

(83) Let V be a bimodule structure over R. Then the following conditions are equivalent:

(i) for all scalars x, y of R and for all vectors v, w of V holds $x \cdot (v + w) = x \cdot v + x \cdot w$ and $(x + y) \cdot v = x \cdot v + y \cdot v$ and $(x \cdot y) \cdot v = x \cdot (y \cdot v)$ and $(1_R) \cdot v = v$ and $(v + w) \cdot x = v \cdot x + w \cdot x$ and $v \cdot (x + y) = v \cdot x + v \cdot y$ and $v \cdot (y \cdot x) = (v \cdot y) \cdot x$ and $v \cdot (1_R) = v$ and $x \cdot (v \cdot y) = (x \cdot v) \cdot y$,
(ii) V is a bimodule over R.

(84) BiMod(R) is a bimodule over R.

Let us consider R. Then BiMod(R) is a bimodule over R.

For simplicity we follow the rules: R will be an associative ring, x, y will be scalars of R, R_2 will be a bimodule over R, and v, w will be vectors of R_2. The following propositions are true:

(85) $x \cdot (v + w) = x \cdot v + x \cdot w$.

(86) $(x + y) \cdot v = x \cdot v + y \cdot v$.

(87) $(x \cdot y) \cdot v = x \cdot (y \cdot v)$.

(88) $(1_R) \cdot v = v$.

(89) $(v + w) \cdot x = v \cdot x + w \cdot x$.

(90) $v \cdot (x + y) = v \cdot x + v \cdot y$.

(91) $v \cdot (y \cdot x) = (v \cdot y) \cdot x$.

(92) $v \cdot (1_R) = v$.

(93) $x \cdot (v \cdot y) = (x \cdot v) \cdot y.$

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] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

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

[7] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

[8] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[9] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[10] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

[11] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received June 20, 1990