

\mathbb{Z} -modules

Yuichi Futa
Shinshu University
Nagano, Japan

Hiroyuki Okazaki¹
Shinshu University
Nagano, Japan

Yasunari Shidama²
Shinshu University
Nagano, Japan

Summary. In this article, we formalize \mathbb{Z} -module, that is a module over integer ring. \mathbb{Z} -module is necessary for lattice problems, LLL (Lenstra-Lenstra-Lovász) base reduction algorithm and cryptographic systems with lattices [11].

MML identifier: ZMODUL01, version: 7.12.01 4.167.1133

The papers [10], [17], [18], [7], [2], [9], [14], [8], [6], [13], [5], [1], [15], [4], [3], [19], [16], and [12] provide the terminology and notation for this paper.

1. DEFINITION OF \mathbb{Z} -MODULE

We introduce \mathbb{Z} -module structures which are extensions of additive loop structure and are systems

\langle a carrier, a zero, an addition, an external multiplication \rangle ,
where the carrier is a set, the zero is an element of the carrier, the addition is a binary operation on the carrier, and the external multiplication is a function from $\mathbb{Z} \times$ the carrier into the carrier.

Let us mention that there exists a \mathbb{Z} -module structure which is non empty.

Let V be a \mathbb{Z} -module structure. A vector of V is an element of V .

In the sequel V denotes a non empty \mathbb{Z} -module structure and v denotes a vector of V .

Let us consider V , v and let a be an integer number. The functor $a \cdot v$ yields an element of V and is defined by:

(Def. 1) $a \cdot v =$ (the external multiplication of V)(a, v).

¹This work was supported by JSPS KAKENHI 21240001.

²This work was supported by JSPS KAKENHI 22300285.

Let Z_1 be a non empty set, let O be an element of Z_1 , let F be a binary operation on Z_1 , and let G be a function from $\mathbb{Z} \times Z_1$ into Z_1 . One can verify that $\langle Z_1, O, F, G \rangle$ is non empty.

Let I_1 be a non empty \mathbb{Z} -module structure. We say that I_1 is vector distributive if and only if:

(Def. 2) For every a and for all vectors v, w of I_1 holds $a \cdot (v + w) = a \cdot v + a \cdot w$.

We say that I_1 is scalar distributive if and only if:

(Def. 3) For all a, b and for every vector v of I_1 holds $(a + b) \cdot v = a \cdot v + b \cdot v$.

We say that I_1 is scalar associative if and only if:

(Def. 4) For all a, b and for every vector v of I_1 holds $(a \cdot b) \cdot v = a \cdot (b \cdot v)$.

We say that I_1 is scalar unital if and only if:

(Def. 5) For every vector v of I_1 holds $1 \cdot v = v$.

The strict \mathbb{Z} -module structure the trivial structure of \mathbb{Z} -module is defined as follows:

(Def. 6) The trivial structure of \mathbb{Z} -module = $\langle 1, \text{op}_0, \text{op}_2, \pi_2(\mathbb{Z} \times 1) \rangle$.

Let us observe that the trivial structure of \mathbb{Z} -module is trivial and non empty.

Let us observe that there exists a non empty \mathbb{Z} -module structure which is strict, Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, and scalar unital.

A \mathbb{Z} -module is an Abelian add-associative right zeroed right complementable scalar distributive vector distributive scalar associative scalar unital non empty \mathbb{Z} -module structure.

In the sequel v, w denote vectors of V .

Let I_1 be a non empty \mathbb{Z} -module structure. We say that I_1 inherits cancelable on multiplication if and only if:

(Def. 7) For every a and for every vector v of I_1 such that $a \cdot v = 0_{(I_1)}$ holds $a = 0$ or $v = 0_{(I_1)}$.

The following propositions are true:

- (1) If $a = 0$ or $v = 0_V$, then $a \cdot v = 0_V$.
- (2) $-v = (-1) \cdot v$.
- (3) If V inherits cancelable on multiplication and $v = -v$, then $v = 0_V$.
- (4) If V inherits cancelable on multiplication and $v + v = 0_V$, then $v = 0_V$.
- (5) $a \cdot -v = (-a) \cdot v$.
- (6) $a \cdot -v = -a \cdot v$.
- (7) $(-a) \cdot -v = a \cdot v$.
- (8) $a \cdot (v - w) = a \cdot v - a \cdot w$.
- (9) $(a - b) \cdot v = a \cdot v - b \cdot v$.
- (10) If V inherits cancelable on multiplication and $a \neq 0$ and $a \cdot v = a \cdot w$, then $v = w$.

- (11) If V inherits cancelable on multiplication and $v \neq 0_V$ and $a \cdot v = b \cdot v$, then $a = b$.

For simplicity, we follow the rules: V is a \mathbb{Z} -module, u, v, w are vectors of V , F, G, H, I are finite sequences of elements of V , j, k, n are elements of \mathbb{N} , and f_9 is a function from \mathbb{N} into the carrier of V .

Next we state several propositions:

- (12) If $\text{len } F = \text{len } G$ and for all k, v such that $k \in \text{dom } F$ and $v = G(k)$ holds $F(k) = a \cdot v$, then $\sum F = a \cdot \sum G$.
- (13) For every \mathbb{Z} -module V and for every integer a holds $a \cdot \sum(\varepsilon_{(\text{the carrier of } V)}) = 0_V$.
- (14) For every \mathbb{Z} -module V and for every integer a and for all vectors v, u of V holds $a \cdot \sum\langle v, u \rangle = a \cdot v + a \cdot u$.
- (15) For every \mathbb{Z} -module V and for every integer a and for all vectors v, u, w of V holds $a \cdot \sum\langle v, u, w \rangle = a \cdot v + a \cdot u + a \cdot w$.
- (16) $(-a) \cdot v = -a \cdot v$.
- (17) If $\text{len } F = \text{len } G$ and for every k such that $k \in \text{dom } F$ holds $G(k) = a \cdot F_k$, then $\sum G = a \cdot \sum F$.

2. SUBMODULES AND COSETS OF SUBMODULES IN \mathbb{Z} -MODULE

We use the following convention: V, X are \mathbb{Z} -modules, V_1, V_2, V_3 are subsets of V , and x is a set.

Let us consider V, V_1 . We say that V_1 is linearly closed if and only if:

- (Def. 8) For all v, u such that $v, u \in V_1$ holds $v + u \in V_1$ and for all a, v such that $v \in V_1$ holds $a \cdot v \in V_1$.

One can prove the following propositions:

- (18) If $V_1 \neq \emptyset$ and V_1 is linearly closed, then $0_V \in V_1$.
- (19) If V_1 is linearly closed, then for every v such that $v \in V_1$ holds $-v \in V_1$.
- (20) If V_1 is linearly closed, then for all v, u such that $v, u \in V_1$ holds $v - u \in V_1$.
- (21) If the carrier of $V = V_1$, then V_1 is linearly closed.
- (22) If V_1 is linearly closed and V_2 is linearly closed and $V_3 = \{v + u : v \in V_1 \wedge u \in V_2\}$, then V_3 is linearly closed.

Let us consider V . Observe that $\{0_V\}$ is linearly closed.

Let us consider V . Note that there exists a subset of V which is linearly closed.

Let us consider V and let V_1, V_2 be linearly closed subsets of V . Note that $V_1 \cap V_2$ is linearly closed.

Let us consider V . A \mathbb{Z} -module is called a submodule of V if it satisfies the conditions (Def. 9).

- (Def. 9)(i) The carrier of $it \subseteq$ the carrier of V ,
- (ii) $0_{it} = 0_V$,
 - (iii) the addition of $it =$ (the addition of V) \upharpoonright (the carrier of it), and
 - (iv) the external multiplication of $it =$ (the external multiplication of V) \upharpoonright ($\mathbb{Z} \times$ the carrier of it).

In the sequel W_2 denotes a submodule of V and w, w_1, w_2 denote vectors of W .

We now state a number of propositions:

- (23) If $x \in W_1$ and W_1 is a submodule of W_2 , then $x \in W_2$.
- (24) If $x \in W$, then $x \in V$.
- (25) w is a vector of V .
- (26) $0_W = 0_V$.
- (27) $0_{(W_1)} = 0_{(W_2)}$.
- (28) If $w_1 = v$ and $w_2 = u$, then $w_1 + w_2 = v + u$.
- (29) If $w = v$, then $a \cdot w = a \cdot v$.
- (30) If $w = v$, then $-v = -w$.
- (31) If $w_1 = v$ and $w_2 = u$, then $w_1 - w_2 = v - u$.
- (32) V is a submodule of V .
- (33) $0_V \in W$.
- (34) $0_{(W_1)} \in W_2$.
- (35) $0_W \in V$.
- (36) If $u, v \in W$, then $u + v \in W$.
- (37) If $v \in W$, then $a \cdot v \in W$.
- (38) If $v \in W$, then $-v \in W$.
- (39) If $u, v \in W$, then $u - v \in W$.

In the sequel d_1 is an element of D , A is a binary operation on D , and M is a function from $\mathbb{Z} \times D$ into D .

We now state several propositions:

- (40) Suppose $V_1 = D$ and $d_1 = 0_V$ and $A =$ (the addition of V) \upharpoonright (V_1) and $M =$ (the external multiplication of V) \upharpoonright ($\mathbb{Z} \times V_1$). Then $\langle D, d_1, A, M \rangle$ is a submodule of V .
- (41) For all strict \mathbb{Z} -modules V, X such that V is a submodule of X and X is a submodule of V holds $V = X$.
- (42) If V is a submodule of X and X is a submodule of Y , then V is a submodule of Y .
- (43) If the carrier of $W_1 \subseteq$ the carrier of W_2 , then W_1 is a submodule of W_2 .
- (44) If for every v such that $v \in W_1$ holds $v \in W_2$, then W_1 is a submodule of W_2 .

Let us consider V . Note that there exists a submodule of V which is strict. Next we state several propositions:

- (45) For all strict submodules W_1, W_2 of V such that the carrier of $W_1 =$ the carrier of W_2 holds $W_1 = W_2$.
- (46) For all strict submodules W_1, W_2 of V such that for every v holds $v \in W_1$ iff $v \in W_2$ holds $W_1 = W_2$.
- (47) Let V be a strict \mathbb{Z} -module and W be a strict submodule of V . If the carrier of $W =$ the carrier of V , then $W = V$.
- (48) Let V be a strict \mathbb{Z} -module and W be a strict submodule of V . If for every vector v of V holds $v \in W$ iff $v \in V$, then $W = V$.
- (49) If the carrier of $W = V_1$, then V_1 is linearly closed.
- (50) If $V_1 \neq \emptyset$ and V_1 is linearly closed, then there exists a strict submodule W of V such that $V_1 =$ the carrier of W .

Let us consider V . The functor $\mathbf{0}_V$ yielding a strict submodule of V is defined by:

- (Def. 10) The carrier of $\mathbf{0}_V = \{0_V\}$.

Let us consider V . The functor Ω_V yields a strict submodule of V and is defined by:

- (Def. 11) $\Omega_V =$ the \mathbb{Z} -module structure of V .

We now state several propositions:

- (51) $\mathbf{0}_W = \mathbf{0}_V$.
- (52) $\mathbf{0}_{(W_1)} = \mathbf{0}_{(W_2)}$.
- (53) $\mathbf{0}_W$ is a submodule of V .
- (54) $\mathbf{0}_V$ is a submodule of W .
- (55) $\mathbf{0}_{(W_1)}$ is a submodule of W_2 .
- (56) Every strict \mathbb{Z} -module V is a submodule of Ω_V .

Let us consider V, v, W . The functor $v + W$ yields a subset of V and is defined as follows:

- (Def. 12) $v + W = \{v + u : u \in W\}$.

Let us consider V, W . A subset of V is called a coset of W if:

- (Def. 13) There exists v such that it $= v + W$.

In the sequel B, C are cosets of W .

The following propositions are true:

- (57) $0_V \in v + W$ iff $v \in W$.
- (58) $v \in v + W$.
- (59) $0_V + W =$ the carrier of W .
- (60) $v + \mathbf{0}_V = \{v\}$.
- (61) $v + \Omega_V =$ the carrier of V .

- (62) $0_V \in v + W$ iff $v + W =$ the carrier of W .
- (63) $v \in W$ iff $v + W =$ the carrier of W .
- (64) If $v \in W$, then $a \cdot v + W =$ the carrier of W .
- (65) $u \in W$ iff $v + W = v + u + W$.
- (66) $u \in W$ iff $v + W = (v - u) + W$.
- (67) $v \in u + W$ iff $u + W = v + W$.
- (68) If $u \in v_1 + W$ and $u \in v_2 + W$, then $v_1 + W = v_2 + W$.
- (69) If $v \in W$, then $a \cdot v \in v + W$.
- (70) $u + v \in v + W$ iff $u \in W$.
- (71) $v - u \in v + W$ iff $u \in W$.
- (72) $u \in v + W$ iff there exists v_1 such that $v_1 \in W$ and $u = v + v_1$.
- (73) $u \in v + W$ iff there exists v_1 such that $v_1 \in W$ and $u = v - v_1$.
- (74) There exists v such that $v_1, v_2 \in v + W$ iff $v_1 - v_2 \in W$.
- (75) If $v + W = u + W$, then there exists v_1 such that $v_1 \in W$ and $v + v_1 = u$.
- (76) If $v + W = u + W$, then there exists v_1 such that $v_1 \in W$ and $v - v_1 = u$.
- (77) For all strict submodules W_1, W_2 of V such that $v + W_1 = v + W_2$ holds $W_1 = W_2$.
- (78) For all strict submodules W_1, W_2 of V such that $v + W_1 = u + W_2$ holds $W_1 = W_2$.
- (79) C is linearly closed iff $C =$ the carrier of W .
- (80) For all strict submodules W_1, W_2 of V and for every coset C_1 of W_1 and for every coset C_2 of W_2 such that $C_1 = C_2$ holds $W_1 = W_2$.
- (81) $\{v\}$ is a coset of $\mathbf{0}_V$.
- (82) If V_1 is a coset of $\mathbf{0}_V$, then there exists v such that $V_1 = \{v\}$.
- (83) The carrier of W is a coset of W .
- (84) The carrier of V is a coset of Ω_V .
- (85) If V_1 is a coset of Ω_V , then $V_1 =$ the carrier of V .
- (86) $0_V \in C$ iff $C =$ the carrier of W .
- (87) $u \in C$ iff $C = u + W$.
- (88) If $u, v \in C$, then there exists v_1 such that $v_1 \in W$ and $u + v_1 = v$.
- (89) If $u, v \in C$, then there exists v_1 such that $v_1 \in W$ and $u - v_1 = v$.
- (90) There exists C such that $v_1, v_2 \in C$ iff $v_1 - v_2 \in W$.
- (91) If $u \in B$ and $u \in C$, then $B = C$.

3. OPERATIONS ON SUBMODULES IN \mathbb{Z} -MODULE

For simplicity, we use the following convention: V is a \mathbb{Z} -module, W, W_1, W_2, W_3 are submodules of V , u, u_1, u_2, v, v_1, v_2 are vectors of V , a, a_1, a_2 are integer numbers, and X, Y, y, y_1, y_2 are sets.

Let us consider V, W_1, W_2 . The functor $W_1 + W_2$ yielding a strict submodule of V is defined by:

(Def. 14) The carrier of $W_1 + W_2 = \{v + u : v \in W_1 \wedge u \in W_2\}$.

Let us notice that the functor $W_1 + W_2$ is commutative.

Let us consider V, W_1, W_2 . The functor $W_1 \cap W_2$ yields a strict submodule of V and is defined as follows:

(Def. 15) The carrier of $W_1 \cap W_2 = (\text{the carrier of } W_1) \cap (\text{the carrier of } W_2)$.

Let us observe that the functor $W_1 \cap W_2$ is commutative.

We now state a number of propositions:

(92) $x \in W_1 + W_2$ iff there exist v_1, v_2 such that $v_1 \in W_1$ and $v_2 \in W_2$ and $x = v_1 + v_2$.

(93) If $v \in W_1$ or $v \in W_2$, then $v \in W_1 + W_2$.

(94) $x \in W_1 \cap W_2$ iff $x \in W_1$ and $x \in W_2$.

(95) For every strict submodule W of V holds $W + W = W$.

(96) $W_1 + (W_2 + W_3) = (W_1 + W_2) + W_3$.

(97) W_1 is a submodule of $W_1 + W_2$.

(98) For every strict submodule W_2 of V holds W_1 is a submodule of W_2 iff $W_1 + W_2 = W_2$.

(99) For every strict submodule W of V holds $\mathbf{0}_V + W = W$.

(100) $\mathbf{0}_V + \Omega_V =$ the \mathbb{Z} -module structure of V .

(101) $\Omega_V + W =$ the \mathbb{Z} -module structure of V .

(102) For every strict \mathbb{Z} -module V holds $\Omega_V + \Omega_V = V$.

(103) For every strict submodule W of V holds $W \cap W = W$.

(104) $W_1 \cap (W_2 \cap W_3) = (W_1 \cap W_2) \cap W_3$.

(105) $W_1 \cap W_2$ is a submodule of W_1 .

(106) For every strict submodule W_1 of V holds W_1 is a submodule of W_2 iff $W_1 \cap W_2 = W_1$.

(107) $\mathbf{0}_V \cap W = \mathbf{0}_V$.

(108) $\mathbf{0}_V \cap \Omega_V = \mathbf{0}_V$.

(109) For every strict submodule W of V holds $\Omega_V \cap W = W$.

(110) For every strict \mathbb{Z} -module V holds $\Omega_V \cap \Omega_V = V$.

(111) $W_1 \cap W_2$ is a submodule of $W_1 + W_2$.

(112) For every strict submodule W_2 of V holds $W_1 \cap W_2 + W_2 = W_2$.

- (113) For every strict submodule W_1 of V holds $W_1 \cap (W_1 + W_2) = W_1$.
- (114) $W_1 \cap W_2 + W_2 \cap W_3$ is a submodule of $W_2 \cap (W_1 + W_3)$.
- (115) If W_1 is a submodule of W_2 , then $W_2 \cap (W_1 + W_3) = W_1 \cap W_2 + W_2 \cap W_3$.
- (116) $W_2 + W_1 \cap W_3$ is a submodule of $(W_1 + W_2) \cap (W_2 + W_3)$.
- (117) If W_1 is a submodule of W_2 , then $W_2 + W_1 \cap W_3 = (W_1 + W_2) \cap (W_2 + W_3)$.
- (118) If W_1 is a strict submodule of W_3 , then $W_1 + W_2 \cap W_3 = (W_1 + W_2) \cap W_3$.
- (119) For all strict submodules W_1, W_2 of V holds $W_1 + W_2 = W_2$ iff $W_1 \cap W_2 = W_1$.
- (120) For all strict submodules W_2, W_3 of V such that W_1 is a submodule of W_2 holds $W_1 + W_3$ is a submodule of $W_2 + W_3$.
- (121) There exists W such that the carrier of $W = (\text{the carrier of } W_1) \cup (\text{the carrier of } W_2)$ if and only if W_1 is a submodule of W_2 or W_2 is a submodule of W_1 .

Let us consider V . The functor $\text{Sub}(V)$ yields a set and is defined by:

- (Def. 16) For every x holds $x \in \text{Sub}(V)$ iff x is a strict submodule of V .

Let us consider V . One can verify that $\text{Sub}(V)$ is non empty.

We now state the proposition

- (122) For every strict \mathbb{Z} -module V holds $V \in \text{Sub}(V)$.

Let us consider V, W_1, W_2 . We say that V is the direct sum of W_1 and W_2 if and only if:

- (Def. 17) The \mathbb{Z} -module structure of $V = W_1 + W_2$ and $W_1 \cap W_2 = \mathbf{0}_V$.

Let V be a \mathbb{Z} -module and let W be a submodule of V . We say that W has linear complement if and only if:

- (Def. 18) There exists a submodule C of V such that V is the direct sum of C and W .

Let V be a \mathbb{Z} -module. Observe that there exists a submodule of V which has linear complement.

Let V be a \mathbb{Z} -module and let W be a submodule of V . Let us assume that W has linear complement. A submodule of V is called a linear complement of W if:

- (Def. 19) V is the direct sum of it and W .

One can prove the following propositions:

- (123) Let V be a \mathbb{Z} -module and W_1, W_2 be submodules of V . Suppose V is the direct sum of W_1 and W_2 . Then W_2 is a linear complement of W_1 .
- (124) Let V be a \mathbb{Z} -module, W be a submodule of V with linear complement, and L be a linear complement of W . Then V is the direct sum of L and W and the direct sum of W and L .

- (125) Let V be a \mathbb{Z} -module, W be a submodule of V with linear complement, and L be a linear complement of W . Then $W + L =$ the \mathbb{Z} -module structure of V .
- (126) Let V be a \mathbb{Z} -module, W be a submodule of V with linear complement, and L be a linear complement of W . Then $W \cap L = \mathbf{0}_V$.
- (127) If V is the direct sum of W_1 and W_2 , then V is the direct sum of W_2 and W_1 .
- (128) Let V be a \mathbb{Z} -module, W be a submodule of V with linear complement, and L be a linear complement of W . Then W is a linear complement of L .
- (129) Every \mathbb{Z} -module V is the direct sum of $\mathbf{0}_V$ and Ω_V and the direct sum of Ω_V and $\mathbf{0}_V$.
- (130) For every \mathbb{Z} -module V holds $\mathbf{0}_V$ is a linear complement of Ω_V and Ω_V is a linear complement of $\mathbf{0}_V$.

In the sequel C is a coset of W , C_1 is a coset of W_1 , and C_2 is a coset of W_2 . Next we state several propositions:

- (131) If C_1 meets C_2 , then $C_1 \cap C_2$ is a coset of $W_1 \cap W_2$.
- (132) Let V be a \mathbb{Z} -module and W_1, W_2 be submodules of V . Then V is the direct sum of W_1 and W_2 if and only if for every coset C_1 of W_1 and for every coset C_2 of W_2 there exists a vector v of V such that $C_1 \cap C_2 = \{v\}$.
- (133) Let V be a \mathbb{Z} -module and W_1, W_2 be submodules of V . Then $W_1 + W_2 =$ the \mathbb{Z} -module structure of V if and only if for every vector v of V there exist vectors v_1, v_2 of V such that $v_1 \in W_1$ and $v_2 \in W_2$ and $v = v_1 + v_2$.
- (134) If V is the direct sum of W_1 and W_2 and $v_1 + v_2 = u_1 + u_2$ and $v_1, u_1 \in W_1$ and $v_2, u_2 \in W_2$, then $v_1 = u_1$ and $v_2 = u_2$.
- (135) Suppose $V = W_1 + W_2$ and there exists v such that for all v_1, v_2, u_1, u_2 such that $v_1 + v_2 = u_1 + u_2$ and $v_1, u_1 \in W_1$ and $v_2, u_2 \in W_2$ holds $v_1 = u_1$ and $v_2 = u_2$. Then V is the direct sum of W_1 and W_2 .

Let us consider V, v, W_1, W_2 . Let us assume that V is the direct sum of W_1 and W_2 . The functor $v_{\langle W_1, W_2 \rangle}$ yields an element of (the carrier of V) \times (the carrier of V) and is defined as follows:

(Def. 20) $v = (v_{\langle W_1, W_2 \rangle})_1 + (v_{\langle W_1, W_2 \rangle})_2$ and $(v_{\langle W_1, W_2 \rangle})_1 \in W_1$ and $(v_{\langle W_1, W_2 \rangle})_2 \in W_2$.

Next we state several propositions:

- (136) If V is the direct sum of W_1 and W_2 , then $(v_{\langle W_1, W_2 \rangle})_1 = (v_{\langle W_2, W_1 \rangle})_2$.
- (137) If V is the direct sum of W_1 and W_2 , then $(v_{\langle W_1, W_2 \rangle})_2 = (v_{\langle W_2, W_1 \rangle})_1$.
- (138) Let V be a \mathbb{Z} -module, W be a submodule of V with linear complement, L be a linear complement of W , v be a vector of V , and t be an element

of (the carrier of V) \times (the carrier of V). If $t_1 + t_2 = v$ and $t_1 \in W$ and $t_2 \in L$, then $t = v_{\langle W, L \rangle}$.

- (139) Let V be a \mathbb{Z} -module, W be a submodule of V with linear complement, L be a linear complement of W , and v be a vector of V . Then $(v_{\langle W, L \rangle})_1 + (v_{\langle W, L \rangle})_2 = v$.
- (140) Let V be a \mathbb{Z} -module, W be a submodule of V with linear complement, L be a linear complement of W , and v be a vector of V . Then $(v_{\langle W, L \rangle})_1 \in W$ and $(v_{\langle W, L \rangle})_2 \in L$.
- (141) Let V be a \mathbb{Z} -module, W be a submodule of V with linear complement, L be a linear complement of W , and v be a vector of V . Then $(v_{\langle W, L \rangle})_1 = (v_{\langle L, W \rangle})_2$.
- (142) Let V be a \mathbb{Z} -module, W be a submodule of V with linear complement, L be a linear complement of W , and v be a vector of V . Then $(v_{\langle W, L \rangle})_2 = (v_{\langle L, W \rangle})_1$.

In the sequel A_1, A_2, B are elements of $\text{Sub}(V)$.

Let us consider V . The functor $\text{SubJoin } V$ yielding a binary operation on $\text{Sub}(V)$ is defined by:

- (Def. 21) For all A_1, A_2, W_1, W_2 such that $A_1 = W_1$ and $A_2 = W_2$ holds $(\text{SubJoin } V)(A_1, A_2) = W_1 + W_2$.

Let us consider V . The functor $\text{SubMeet } V$ yields a binary operation on $\text{Sub}(V)$ and is defined by:

- (Def. 22) For all A_1, A_2, W_1, W_2 such that $A_1 = W_1$ and $A_2 = W_2$ holds $(\text{SubMeet } V)(A_1, A_2) = W_1 \cap W_2$.

One can prove the following proposition

- (143) $\langle \text{Sub}(V), \text{SubJoin } V, \text{SubMeet } V \rangle$ is a lattice.

Let us consider V . Note that $\langle \text{Sub}(V), \text{SubJoin } V, \text{SubMeet } V \rangle$ is lattice-like.

We now state several propositions:

- (144) For every \mathbb{Z} -module V holds $\langle \text{Sub}(V), \text{SubJoin } V, \text{SubMeet } V \rangle$ is lower-bounded.
- (145) For every \mathbb{Z} -module V holds $\langle \text{Sub}(V), \text{SubJoin } V, \text{SubMeet } V \rangle$ is upper-bounded.
- (146) For every \mathbb{Z} -module V holds $\langle \text{Sub}(V), \text{SubJoin } V, \text{SubMeet } V \rangle$ is a bound lattice.
- (147) For every \mathbb{Z} -module V holds $\langle \text{Sub}(V), \text{SubJoin } V, \text{SubMeet } V \rangle$ is modular.
- (148) Let V be a \mathbb{Z} -module and W_1, W_2, W_3 be strict submodules of V . If W_1 is a submodule of W_2 , then $W_1 \cap W_3$ is a submodule of $W_2 \cap W_3$.
- (149) Let V be a \mathbb{Z} -module and W be a strict submodule of V . Suppose that for every vector v of V holds $v \in W$. Then $W =$ the \mathbb{Z} -module structure

of V .

- (150) There exists C such that $v \in C$.

4. TRANSFORMATION OF ABELIAN GROUP TO \mathbb{Z} -MODULE

Let A_3 be a non empty additive loop structure. The left integer multiplication of A_3 yielding a function from $\mathbb{Z} \times$ the carrier of A_3 into the carrier of A_3 is defined by the condition (Def. 23).

(Def. 23) Let i be an element of \mathbb{Z} and a be an element of A_3 . Then

- (i) if $i \geq 0$, then (the left integer multiplication of A_3)(i, a) = (Nat-mult-left A_3)(i, a), and
- (ii) if $i < 0$, then (the left integer multiplication of A_3)(i, a) = (Nat-mult-left A_3)($-i, -a$).

The following propositions are true:

- (151) Let R be a non empty additive loop structure, a be an element of R , i be an element of \mathbb{Z} , and i_1 be an element of \mathbb{N} . If $i = i_1$, then (the left integer multiplication of R)(i, a) = $i_1 \cdot a$.
- (152) Let R be a non empty additive loop structure, a be an element of R , and i be an element of \mathbb{Z} . If $i = 0$, then (the left integer multiplication of R)(i, a) = 0_R .
- (153) Let R be an add-associative right zeroed right complementable non empty additive loop structure and i be an element of \mathbb{N} . Then (Nat-mult-left R)($i, 0_R$) = 0_R .
- (154) Let R be an add-associative right zeroed right complementable non empty additive loop structure and i be an element of \mathbb{Z} . Then (the left integer multiplication of R)($i, 0_R$) = 0_R .
- (155) Let R be a right zeroed non empty additive loop structure, a be an element of R , and i be an element of \mathbb{Z} . If $i = 1$, then (the left integer multiplication of R)(i, a) = a .
- (156) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R , and i, j, k be elements of \mathbb{N} . If $i \leq j$ and $k = j - i$, then (Nat-mult-left R)(k, a) = (Nat-mult-left R)(j, a) - (Nat-mult-left R)(i, a).
- (157) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R , and i be an element of \mathbb{N} . Then -(Nat-mult-left R)(i, a) = (Nat-mult-left R)($i, -a$).
- (158) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R , and i, j be elements of \mathbb{Z} . Suppose $i \in \mathbb{N}$ and $j \notin \mathbb{N}$. Then (the left integer multipli-

cation of $R)(i + j, a) =$ (the left integer multiplication of $R)(i, a) +$ (the left integer multiplication of $R)(j, a)$.

- (159) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R , and i, j be elements of \mathbb{Z} . Then (the left integer multiplication of $R)(i + j, a) =$ (the left integer multiplication of $R)(i, a) +$ (the left integer multiplication of $R)(j, a)$.
- (160) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a, b be elements of R , and i be an element of \mathbb{N} . Then $(\text{Nat-mult-left } R)(i, a + b) = (\text{Nat-mult-left } R)(i, a) + (\text{Nat-mult-left } R)(i, b)$.
- (161) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a, b be elements of R , and i be an element of \mathbb{Z} . Then (the left integer multiplication of $R)(i, a + b) =$ (the left integer multiplication of $R)(i, a) +$ (the left integer multiplication of $R)(i, b)$.
- (162) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R , and i, j be elements of \mathbb{N} . Then $(\text{Nat-mult-left } R)(i \cdot j, a) = (\text{Nat-mult-left } R)(i, (\text{Nat-mult-left } R)(j, a))$.
- (163) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R , and i, j be elements of \mathbb{Z} . Then (the left integer multiplication of $R)(i \cdot j, a) =$ (the left integer multiplication of $R)(i, (\text{the left integer multiplication of } R)(j, a))$.
- (164) Let A_3 be a non empty Abelian add-associative right zeroed right complementable additive loop structure. Then \langle the carrier of A_3 , the zero of A_3 , the addition of A_3 , the left integer multiplication of $A_3\rangle$ is a \mathbb{Z} -module.

REFERENCES

- [1] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(3):537–541, 1990.
- [2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(1):91–96, 1990.
- [3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(1):107–114, 1990.
- [4] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(3):433–439, 1990.
- [5] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(1):245–254, 1990.
- [6] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(1):175–180, 1990.
- [7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(1):153–164, 1990.
- [9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(2):357–367, 1990.
- [10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(1):47–53, 1990.

- [11] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: A cryptographic perspective (the international series in engineering and computer science). 2002.
- [12] Christoph Schwarzweiler. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.
- [13] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
- [14] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
- [15] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
- [16] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
- [17] Żinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
- [18] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
- [19] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Received May 8, 2011
