FORMALIZED MATHEMATICS
Volume 9, Number 3, 2001
University of Białystok

Ring Ideals

Jonathan Backer[1]
University of Alberta
Edmonton

Piotr Rudnicki[2]
University of Alberta
Edmonton

Christoph Schwarzweller[3]
University of Tübingen

Summary. We introduce the basic notions of ideal theory in rings. This includes left and right ideals, (finitely) generated ideals and some operations on ideals such as the addition of ideals and the radical of an ideal. In addition we introduce linear combinations to formalize the well-known characterization of generated ideals. Principal ideal domains and Noetherian rings are defined. The latter development follows [3], pages 144–145.

MML Identifier: IDEAL_1.

The terminology and notation used here are introduced in the following articles: [11], [18], [17], [20], [2], [23], [8], [4], [5], [15], [22], [19], [16], [21], [1], [13], [6], [14], [12], [26], [24], [25], [9], [10], and [7].

1. Preliminaries

Let us note that there exists a non empty loop structure which is add-associative, left zeroed, and right zeroed.

Let us observe that there exists a non empty double loop structure which is Abelian, left zeroed, right zeroed, add-cancelable, well unital, add-associative, associative, commutative, distributive, and non trivial.

One can prove the following proposition

[1]Partially supported by NSERC grant OGP9207.
[2]Partially supported by NSERC grant OGP9207.
[3]Partially supported by CALCULEMUS grant HPRN-CT-2000-00102.

ISSN 1426–2630

(1) Let V be an add-associative left zeroed right zeroed non empty loop structure and v, u be elements of V. Then $\sum\langle v, u\rangle = v + u$.

2. Ideals

Let L be a non empty loop structure and let F be a subset of L. We say that F is add closed if and only if:

(Def. 1) For all elements x, y of the carrier of L such that $x \in F$ and $y \in F$ holds $x + y \in F$.

Let L be a non empty groupoid and let F be a subset of L. We say that F is left ideal if and only if:

(Def. 2) For all elements p, x of the carrier of L such that $x \in F$ holds $p \cdot x \in F$.

We say that F is right ideal if and only if:

(Def. 3) For all elements p, x of the carrier of L such that $x \in F$ holds $x \cdot p \in F$.

Let L be a non empty loop structure. Observe that there exists a non empty subset of L which is add closed.

Let L be a non empty groupoid. One can verify that there exists a non empty subset of L which is left ideal and there exists a non empty subset of L which is right ideal.

Let L be a non empty double loop structure. One can verify the following observations:

* there exists a non empty subset of L which is add closed, left ideal, and right ideal,
* there exists a non empty subset of L which is add closed and right ideal, and
* there exists a non empty subset of L which is add closed and left ideal.

Let R be a commutative non empty groupoid. Observe that every non empty subset of R which is left ideal is also right ideal and every non empty subset of R which is right ideal is also left ideal.

Let L be a non empty double loop structure. An ideal of L is an add closed left ideal right ideal non empty subset of L.

Let L be a non empty double loop structure. A right ideal of L is an add closed right ideal non empty subset of L.

Let L be a non empty double loop structure. A left ideal of L is an add closed left ideal non empty subset of L.

The following propositions are true:

(2) Let R be a right zeroed add-left-cancelable left distributive non empty double loop structure and I be a left ideal non empty subset of R. Then $0_R \in I$.

(3) Let R be a left zeroed add-right-cancelable right distributive non empty double loop structure and I be a right ideal non empty subset of R. Then $0_R \in I$.

(4) For every right zeroed non empty double loop structure L holds $\{0_L\}$ is add closed.

(5) Let L be a left zeroed add-right-cancelable right distributive non empty double loop structure. Then $\{0_L\}$ is left ideal.

(6) Let L be a right zeroed add-left-cancelable left distributive non empty double loop structure. Then $\{0_L\}$ is right ideal.

(7) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure. Then $\{0_L\}$ is an ideal of L.

(8) Let L be an add-associative right zeroed right complementable right distributive non empty double loop structure. Then $\{0_L\}$ is a left ideal of L.

(9) Let L be an add-associative right zeroed right complementable left distributive non empty double loop structure. Then $\{0_L\}$ is a right ideal of L.

(10) For every non empty double loop structure L holds the carrier of L is an ideal of L.

(11) For every non empty double loop structure L holds the carrier of L is a left ideal of L.

(12) For every non empty double loop structure L holds the carrier of L is a right ideal of L.

Let R be a left zeroed right zeroed add-cancelable distributive non empty double loop structure and let I be an ideal of R. Let us observe that I is trivial if and only if:

(Def. 4) $I = \{0_R\}$.

Let S be a 1-sorted structure and let T be a subset of S. We say that T is proper if and only if:

(Def. 5) $T \neq$ the carrier of S.

Let S be a non empty 1-sorted structure. Note that there exists a subset of S which is proper.

Let R be a non trivial left zeroed right zeroed add-cancelable distributive non empty double loop structure. One can check that there exists an ideal of R which is proper.

The following propositions are true:

(13) Let L be an add-associative right zeroed right complementable left distributive left unital non empty double loop structure, I be a left ideal non empty subset of L, and x be an element of the carrier of L. If $x \in I$, then $-x \in I$.

(14) Let L be an add-associative right zeroed right complementable right distributive right unital non empty double loop structure, I be a right ideal non empty subset of L, and x be an element of the carrier of L. If $x \in I$, then $-x \in I$.

(15) Let L be an add-associative right zeroed right complementable left distributive left unital non empty double loop structure, I be a left ideal of L, and x, y be elements of the carrier of L. If $x \in I$ and $y \in I$, then $x - y \in I$.

(16) Let L be an add-associative right zeroed right complementable right distributive right unital non empty double loop structure, I be a right ideal of L, and x, y be elements of the carrier of L. If $x \in I$ and $y \in I$, then $x - y \in I$.

(17) Let R be a left zeroed right zeroed add-cancelable add-associative distributive non empty double loop structure, I be an add closed right ideal non empty subset of R, a be an element of I, and n be a natural number. Then $n \cdot a \in I$.

(18) Let R be a unital left zeroed right zeroed add-cancelable associative distributive non empty double loop structure, I be a right ideal non empty subset of R, a be an element of I, and n be a natural number. If $n \neq 0$, then $a^n \in I$.

Let R be a non empty loop structure and let I be an add closed non empty subset of R. The functor $\mathrm{add}\,|(I, R)$ yielding a binary operation on I is defined as follows:

(Def. 6) $\mathrm{add}\,|(I, R) = (\text{the addition of } R) \restriction [: I, I :]$.

Let R be a non empty groupoid and let I be a right ideal non empty subset of R. The functor $\mathrm{mult}\,|(I, R)$ yielding a binary operation on I is defined as follows:

(Def. 7) $\mathrm{mult}\,|(I, R) = (\text{the multiplication of } R) \restriction [: I, I :]$.

Let R be a non empty loop structure and let I be an add closed non empty subset of R. The functor $\mathrm{Gr}(I, R)$ yields a non empty loop structure and is defined by:

(Def. 8) $\mathrm{Gr}(I, R) = \langle I, \mathrm{add}\,|(I, R), 0_R (\in I)\rangle$.

Let R be a left zeroed right zeroed add-cancelable add-associative distributive non empty double loop structure and let I be an add closed non empty subset of R. Note that $\mathrm{Gr}(I, R)$ is add-associative.

Let R be a left zeroed right zeroed add-cancelable add-associative distributive non empty double loop structure and let I be an add closed right ideal non empty subset of R. Observe that $\mathrm{Gr}(I, R)$ is right zeroed.

Let R be an Abelian non empty double loop structure and let I be an add closed non empty subset of R. Observe that $\mathrm{Gr}(I, R)$ is Abelian.

Let R be an Abelian right unital left zeroed right zeroed right complementable add-associative distributive non empty double loop structure and let I be an add closed right ideal non empty subset of R. Note that $\mathrm{Gr}(I, R)$ is right complementable.

We now state four propositions:

(19) Let R be a right unital non empty double loop structure and I be a left ideal non empty subset of R. Then I is proper if and only if $\mathbf{1}_R \notin I$.

(20) Let R be a left unital right unital non empty double loop structure and I be a right ideal non empty subset of R. Then I is proper if and only if for every element u of R such that u is unital holds $u \notin I$.

(21) Let R be a right unital non empty double loop structure and I be a left ideal right ideal non empty subset of R. Then I is proper if and only if for every element u of R such that u is unital holds $u \notin I$.

(22) Let R be a non degenerated commutative ring. Then R is a field if and only if for every ideal I of R holds $I = \{0_R\}$ or $I =$ the carrier of R.

3. Linear Combinations

Let R be a non empty multiplicative loop structure and let A be a non empty subset of the carrier of R. A finite sequence of elements of the carrier of R is said to be a linear combination of A if:

(Def. 9) For every set i such that $i \in \mathrm{dom}\,\mathrm{it}$ there exist elements u, v of R and there exists an element a of A such that $\mathrm{it}_i = u \cdot a \cdot v$.

A finite sequence of elements of the carrier of R is said to be a left linear combination of A if:

(Def. 10) For every set i such that $i \in \mathrm{dom}\,\mathrm{it}$ there exists an element u of R and there exists an element a of A such that $\mathrm{it}_i = u \cdot a$.

A finite sequence of elements of the carrier of R is said to be a right linear combination of A if:

(Def. 11) For every set i such that $i \in \mathrm{dom}\,\mathrm{it}$ there exists an element u of R and there exists an element a of A such that $\mathrm{it}_i = a \cdot u$.

Let R be a non empty multiplicative loop structure and let A be a non empty subset of the carrier of R. One can verify the following observations:

* there exists a linear combination of A which is non empty,
* there exists a left linear combination of A which is non empty, and
* there exists a right linear combination of A which is non empty.

Let R be a non empty multiplicative loop structure, let A, B be non empty subsets of the carrier of R, let F be a linear combination of A, and let G be a linear combination of B. Then $F \frown G$ is a linear combination of $A \cup B$.

One can prove the following three propositions:

(23) Let R be an associative non empty multiplicative loop structure, A be a non empty subset of the carrier of R, a be an element of the carrier of R, and F be a linear combination of A. Then $a \cdot F$ is a linear combination of A.

(24) Let R be an associative non empty multiplicative loop structure, A be a non empty subset of the carrier of R, a be an element of the carrier of R, and F be a linear combination of A. Then $F \cdot a$ is a linear combination of A.

(25) Let R be a right unital non empty multiplicative loop structure and A be a non empty subset of the carrier of R. Then every left linear combination of A is a linear combination of A.

Let R be a non empty multiplicative loop structure, let A, B be non empty subsets of the carrier of R, let F be a left linear combination of A, and let G be a left linear combination of B. Then $F \frown G$ is a left linear combination of $A \cup B$.

One can prove the following three propositions:

(26) Let R be an associative non empty multiplicative loop structure, A be a non empty subset of the carrier of R, a be an element of the carrier of R, and F be a left linear combination of A. Then $a \cdot F$ is a left linear combination of A.

(27) Let R be a non empty multiplicative loop structure, A be a non empty subset of the carrier of R, a be an element of the carrier of R, and F be a left linear combination of A. Then $F \cdot a$ is a linear combination of A.

(28) Let R be a left unital non empty multiplicative loop structure and A be a non empty subset of the carrier of R. Then every right linear combination of A is a linear combination of A.

Let R be a non empty multiplicative loop structure, let A, B be non empty subsets of the carrier of R, let F be a right linear combination of A, and let G be a right linear combination of B. Then $F \frown G$ is a right linear combination of $A \cup B$.

Next we state several propositions:

(29) Let R be an associative non empty multiplicative loop structure, A be a non empty subset of the carrier of R, a be an element of the carrier of R, and F be a right linear combination of A. Then $F \cdot a$ is a right linear combination of A.

(30) Let R be an associative non empty multiplicative loop structure, A be a non empty subset of the carrier of R, a be an element of the carrier of R, and F be a right linear combination of A. Then $a \cdot F$ is a linear combination of A.

(31) Let R be a commutative associative non empty multiplicative loop struc-

ture and A be a non empty subset of the carrier of R. Then every linear combination of A is a left linear combination of A and a right linear combination of A.

(32) Let S be a non empty double loop structure, F be a non empty subset of the carrier of S, and l_1 be a non empty linear combination of F. Then there exists a linear combination p of F and there exists an element e of the carrier of S such that $l_1 = p \frown \langle e \rangle$ and $\langle e \rangle$ is a linear combination of F.

(33) Let S be a non empty double loop structure, F be a non empty subset of the carrier of S, and l_1 be a non empty left linear combination of F. Then there exists a left linear combination p of F and there exists an element e of the carrier of S such that $l_1 = p \frown \langle e \rangle$ and $\langle e \rangle$ is a left linear combination of F.

(34) Let S be a non empty double loop structure, F be a non empty subset of the carrier of S, and l_1 be a non empty right linear combination of F. Then there exists a right linear combination p of F and there exists an element e of the carrier of S such that $l_1 = p \frown \langle e \rangle$ and $\langle e \rangle$ is a right linear combination of F.

Let R be a non empty multiplicative loop structure, let A be a non empty subset of the carrier of R, let L be a linear combination of A, and let E be a finite sequence of elements of $[\!:$ the carrier of R, the carrier of R, the carrier of $R\,:\!]$. We say that E represents L if and only if:

(Def. 12) $\operatorname{len} E = \operatorname{len} L$ and for every set i such that $i \in \operatorname{dom} L$ holds $L(i) = (E_i)_{\mathbf{1}} \cdot (E_i)_{\mathbf{2}} \cdot (E_i)_{\mathbf{3}}$ and $(E_i)_{\mathbf{2}} \in A$.

The following propositions are true:

(35) Let R be a non empty multiplicative loop structure, A be a non empty subset of the carrier of R, and L be a linear combination of A. Then there exists a finite sequence E of elements of $[\!:$ the carrier of R, the carrier of R, the carrier of $R\,:\!]$ such that E represents L.

(36) Let R, S be non empty multiplicative loop structures, F be a non empty subset of the carrier of R, l_1 be a linear combination of F, G be a non empty subset of the carrier of S, P be a function from the carrier of R into the carrier of S, and E be a finite sequence of elements of $[\!:$ the carrier of R, the carrier of R, the carrier of $R\,:\!]$. Suppose $P^\circ F \subseteq G$ and E represents l_1. Then there exists a linear combination L_1 of G such that $\operatorname{len} l_1 = \operatorname{len} L_1$ and for every set i such that $i \in \operatorname{dom} L_1$ holds $L_1(i) = P((E_i)_{\mathbf{1}}) \cdot P((E_i)_{\mathbf{2}}) \cdot P((E_i)_{\mathbf{3}})$.

Let R be a non empty multiplicative loop structure, let A be a non empty subset of the carrier of R, let L be a left linear combination of A, and let E be a finite sequence of elements of $[\!:$ the carrier of R, the carrier of $R\,:\!]$. We say that

E represents L if and only if:

(Def. 13) $\operatorname{len} E = \operatorname{len} L$ and for every set i such that $i \in \operatorname{dom} L$ holds $L(i) = (E_i)_{\mathbf{1}} \cdot (E_i)_{\mathbf{2}}$ and $(E_i)_{\mathbf{2}} \in A$.

One can prove the following two propositions:

(37) Let R be a non empty multiplicative loop structure, A be a non empty subset of the carrier of R, and L be a left linear combination of A. Then there exists a finite sequence E of elements of $[\!:$ the carrier of $R,$ the carrier of $R\,:\!]$ such that E represents L.

(38) Let R, S be non empty multiplicative loop structures, F be a non empty subset of the carrier of R, l_1 be a left linear combination of F, G be a non empty subset of the carrier of S, P be a function from the carrier of R into the carrier of S, and E be a finite sequence of elements of $[\!:$ the carrier of $R,$ the carrier of $R\,:\!]$. Suppose $P^{\circ}F \subseteq G$ and E represents l_1. Then there exists a left linear combination L_1 of G such that $\operatorname{len} l_1 = \operatorname{len} L_1$ and for every set i such that $i \in \operatorname{dom} L_1$ holds $L_1(i) = P((E_i)_{\mathbf{1}}) \cdot P((E_i)_{\mathbf{2}})$.

Let R be a non empty multiplicative loop structure, let A be a non empty subset of the carrier of R, let L be a right linear combination of A, and let E be a finite sequence of elements of $[\!:$ the carrier of $R,$ the carrier of $R\,:\!]$. We say that E represents L if and only if:

(Def. 14) $\operatorname{len} E = \operatorname{len} L$ and for every set i such that $i \in \operatorname{dom} L$ holds $L(i) = (E_i)_{\mathbf{1}} \cdot (E_i)_{\mathbf{2}}$ and $(E_i)_{\mathbf{1}} \in A$.

One can prove the following propositions:

(39) Let R be a non empty multiplicative loop structure, A be a non empty subset of the carrier of R, and L be a right linear combination of A. Then there exists a finite sequence E of elements of $[\!:$ the carrier of $R,$ the carrier of $R\,:\!]$ such that E represents L.

(40) Let R, S be non empty multiplicative loop structures, F be a non empty subset of the carrier of R, l_1 be a right linear combination of F, G be a non empty subset of the carrier of S, P be a function from the carrier of R into the carrier of S, and E be a finite sequence of elements of $[\!:$ the carrier of $R,$ the carrier of $R\,:\!]$. Suppose $P^{\circ}F \subseteq G$ and E represents l_1. Then there exists a right linear combination L_1 of G such that $\operatorname{len} l_1 = \operatorname{len} L_1$ and for every set i such that $i \in \operatorname{dom} L_1$ holds $L_1(i) = P((E_i)_{\mathbf{1}}) \cdot P((E_i)_{\mathbf{2}})$.

(41) Let R be a non empty multiplicative loop structure, A be a non empty subset of the carrier of R, l be a linear combination of A, and n be a natural number. Then $l \restriction \operatorname{Seg} n$ is a linear combination of A.

(42) Let R be a non empty multiplicative loop structure, A be a non empty subset of the carrier of R, l be a left linear combination of A, and n be a natural number. Then $l \restriction \operatorname{Seg} n$ is a left linear combination of A.

(43) Let R be a non empty multiplicative loop structure, A be a non empty

subset of the carrier of R, l be a right linear combination of A, and n be a natural number. Then $l \restriction \operatorname{Seg} n$ is a right linear combination of A.

4. Generated Ideals

Let L be a non empty double loop structure and let F be a subset of the carrier of L. Let us assume that F is non empty. The functor F–ideal yielding an ideal of L is defined by:

(Def. 15) $F \subseteq F$–ideal and for every ideal I of L such that $F \subseteq I$ holds F–ideal $\subseteq I$.

The functor F–left-ideal yields a left ideal of L and is defined by:

(Def. 16) $F \subseteq F$–left-ideal and for every left ideal I of L such that $F \subseteq I$ holds F–left-ideal $\subseteq I$.

The functor F–right-ideal yields a right ideal of L and is defined as follows:

(Def. 17) $F \subseteq F$–right-ideal and for every right ideal I of L such that $F \subseteq I$ holds F–right-ideal $\subseteq I$.

One can prove the following three propositions:

(44) For every non empty double loop structure L and for every ideal I of L holds I–ideal $= I$.

(45) For every non empty double loop structure L and for every left ideal I of L holds I–left-ideal $= I$.

(46) For every non empty double loop structure L and for every right ideal I of L holds I–right-ideal $= I$.

Let L be a non empty double loop structure and let I be an ideal of L. A non empty subset of L is said to be a basis of I if:

(Def. 18) It–ideal $= I$.

We now state a number of propositions:

(47) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure. Then $\{0_L\}$–ideal $= \{0_L\}$.

(48) For every left zeroed right zeroed add-cancelable distributive non empty double loop structure L holds $\{0_L\}$–ideal $= \{0_L\}$.

(49) Let L be a left zeroed right zeroed add-right-cancelable right distributive non empty double loop structure. Then $\{0_L\}$–left-ideal $= \{0_L\}$.

(50) For every right zeroed add-left-cancelable left distributive non empty double loop structure L holds $\{0_L\}$–right-ideal $= \{0_L\}$.

(51) For every well unital non empty double loop structure L holds $\{\mathbf{1}_L\}$–ideal $=$ the carrier of L.

(52) For every right unital non empty double loop structure L holds $\{\mathbf{1}_L\}$–left-ideal = the carrier of L.

(53) For every left unital non empty double loop structure L holds $\{\mathbf{1}_L\}$–right-ideal = the carrier of L.

(54) For every non empty double loop structure L holds Ω_L–ideal = the carrier of L.

(55) For every non empty double loop structure L holds Ω_L–left-ideal = the carrier of L.

(56) For every non empty double loop structure L holds Ω_L–right-ideal = the carrier of L.

(57) Let L be a non empty double loop structure and A, B be non empty subsets of the carrier of L. If $A \subseteq B$, then A–ideal $\subseteq$ B–ideal.

(58) Let L be a non empty double loop structure and A, B be non empty subsets of the carrier of L. If $A \subseteq B$, then A–left-ideal $\subseteq$ B–left-ideal.

(59) Let L be a non empty double loop structure and A, B be non empty subsets of the carrier of L. If $A \subseteq B$, then A–right-ideal $\subseteq$ B–right-ideal.

(60) Let L be an add-associative left zeroed right zeroed add-cancelable associative distributive well unital non empty double loop structure, F be a non empty subset of the carrier of L, and x be a set. Then $x \in F$–ideal if and only if there exists a linear combination f of F such that $x = \sum f$.

(61) Let L be an add-associative left zeroed right zeroed add-cancelable associative distributive well unital non empty double loop structure, F be a non empty subset of the carrier of L, and x be a set. Then $x \in F$–left-ideal if and only if there exists a left linear combination f of F such that $x = \sum f$.

(62) Let L be an add-associative left zeroed right zeroed add-cancelable associative distributive well unital non empty double loop structure, F be a non empty subset of the carrier of L, and x be a set. Then $x \in F$–right-ideal if and only if there exists a right linear combination f of F such that $x = \sum f$.

(63) Let R be an add-associative left zeroed right zeroed add-cancelable well unital associative commutative distributive non empty double loop structure and F be a non empty subset of the carrier of R. Then F–ideal = F–left-ideal and F–ideal = F–right-ideal.

(64) Let R be an add-associative left zeroed right zeroed add-cancelable well unital associative commutative distributive non empty double loop structure and a be an element of R. Then $\{a\}$–ideal $= \{a \cdot r : r$ ranges over elements of $R\}$.

(65) Let R be an Abelian left zeroed right zeroed add-cancelable well unital add-associative associative commutative distributive non empty double loop structure and a, b be elements of R. Then $\{a, b\}$–ideal $= \{a \cdot r + b \cdot s : r$

ranges over elements of R, s ranges over elements of $R\}$.

(66) For every non empty double loop structure R and for every element a of R holds $a \in \{a\}$–ideal.

(67) Let R be an Abelian left zeroed right zeroed right complementable add-associative associative commutative distributive well unital non empty double loop structure, A be a non empty subset of R, and a be an element of R. If $a \in A$–ideal, then $\{a\}$–ideal $\subseteq A$–ideal.

(68) For every non empty double loop structure R and for all elements a, b of R holds $a \in \{a, b\}$–ideal and $b \in \{a, b\}$–ideal.

(69) For every non empty double loop structure R and for all elements a, b of R holds $\{a\}$–ideal $\subseteq \{a, b\}$–ideal and $\{b\}$–ideal $\subseteq \{a, b\}$–ideal.

5. Some Operations on Ideals

Let R be a non empty groupoid, let I be a subset of R, and let a be an element of R. The functor $a \cdot I$ yielding a subset of R is defined by:

(Def. 19) $a \cdot I = \{a \cdot i; i$ ranges over elements of R: $i \in I\}$.

Let R be a non empty multiplicative loop structure, let I be a non empty subset of R, and let a be an element of R. Observe that $a \cdot I$ is non empty.

Let R be a distributive non empty double loop structure, let I be an add closed subset of R, and let a be an element of R. Observe that $a \cdot I$ is add closed.

Let R be an associative non empty double loop structure, let I be a right ideal subset of R, and let a be an element of R. One can check that $a \cdot I$ is right ideal.

One can prove the following propositions:

(70) Let R be a right zeroed add-left-cancelable left distributive non empty double loop structure and I be a non empty subset of R. Then $0_R \cdot I = \{0_R\}$.

(71) For every left unital non empty double loop structure R and for every subset I of R holds $\mathbf{1}_R \cdot I = I$.

Let R be a non empty loop structure and let I, J be subsets of R. The functor $I + J$ yielding a subset of R is defined by:

(Def. 20) $I + J = \{a + b; a$ ranges over elements of R, b ranges over elements of R: $a \in I \wedge b \in J\}$.

Let R be a non empty loop structure and let I, J be non empty subsets of R. One can check that $I + J$ is non empty.

Let R be an Abelian non empty loop structure and let I, J be subsets of R. Let us observe that the functor $I + J$ is commutative.

Let R be an Abelian add-associative non empty loop structure and let I, J be add closed subsets of R. Note that $I + J$ is add closed.

Let R be a left distributive non empty double loop structure and let I, J be right ideal subsets of R. Observe that $I + J$ is right ideal.

Let R be a right distributive non empty double loop structure and let I, J be left ideal subsets of R. One can check that $I + J$ is left ideal.

One can prove the following propositions:

(72) For every add-associative non empty loop structure R and for all subsets I, J, K of R holds $I + (J + K) = (I + J) + K$.

(73) Let R be a left zeroed right zeroed add-right-cancelable right distributive non empty double loop structure and I, J be right ideal non empty subsets of R. Then $I \subseteq I + J$.

(74) Let R be a left zeroed add-right-cancelable right distributive non empty double loop structure and I, J be right ideal non empty subsets of R. Then $J \subseteq I + J$.

(75) Let R be a non empty loop structure, I, J be subsets of R, and K be an add closed subset of R. If $I \subseteq K$ and $J \subseteq K$, then $I + J \subseteq K$.

(76) Let R be an Abelian left zeroed right zeroed add-cancelable well unital add-associative associative commutative distributive non empty double loop structure and a, b be elements of R. Then $\{a, b\}$–ideal $= \{a\}$–ideal $+$ $\{b\}$–ideal.

Let R be a non empty 1-sorted structure and let I, J be subsets of R. The functor $I \cap J$ yielding a subset of R is defined as follows:

(Def. 21) $I \cap J = \{x; x$ ranges over elements of R: $x \in I \ \wedge \ x \in J\}$.

Let R be a right zeroed add-left-cancelable left distributive non empty double loop structure and let I, J be left ideal non empty subsets of R. Note that $I \cap J$ is non empty.

Let R be a non empty loop structure and let I, J be add closed subsets of R. Note that $I \cap J$ is add closed.

Let R be a non empty multiplicative loop structure and let I, J be left ideal subsets of R. Observe that $I \cap J$ is left ideal.

Let R be a non empty multiplicative loop structure and let I, J be right ideal subsets of R. Note that $I \cap J$ is right ideal.

One can prove the following four propositions:

(77) For every non empty 1-sorted structure R and for all subsets I, J of R holds $I \cap J \subseteq I$ and $I \cap J \subseteq J$.

(78) For every non empty 1-sorted structure R and for all subsets I, J, K of R holds $I \cap (J \cap K) = (I \cap J) \cap K$.

(79) For every non empty 1-sorted structure R and for all subsets I, J, K of R such that $K \subseteq I$ and $K \subseteq J$ holds $K \subseteq I \cap J$.

(80) Let R be an Abelian left zeroed right zeroed right complementable left unital add-associative left distributive non empty double loop structure, I be an add closed left ideal non empty subset of R, J be a subset of R, and K be a non empty subset of R. If $J \subseteq I$, then $I \cap (J + K) = J + I \cap K$.

Let R be a non empty double loop structure and let I, J be subsets of R. The functor $I * J$ yields a subset of R and is defined by the condition (Def. 22).

(Def. 22) $I * J = \{\sum s; s$ ranges over finite sequences of elements of the carrier of R: $\bigwedge_{i\,:\,\text{natural number}} (1 \leqslant i \ \wedge\ i \leqslant \operatorname{len} s \ \Rightarrow\ \bigvee_{a,b\,:\,\text{element of } R} (s(i) = a \cdot b \ \wedge\ a \in I \ \wedge\ b \in J))\}$.

Let R be a non empty double loop structure and let I, J be subsets of R. Note that $I * J$ is non empty.

Let R be a commutative non empty double loop structure and let I, J be subsets of R. Let us observe that the functor $I * J$ is commutative.

Let R be a right zeroed add-associative non empty double loop structure and let I, J be subsets of R. Note that $I * J$ is add closed.

Let R be a right zeroed add-left-cancelable associative left distributive non empty double loop structure and let I, J be right ideal subsets of R. One can check that $I * J$ is right ideal.

Let R be a left zeroed add-right-cancelable associative right distributive non empty double loop structure and let I, J be left ideal subsets of R. Note that $I * J$ is left ideal.

We now state several propositions:

(81) Let R be a left zeroed right zeroed add-left-cancelable left distributive non empty double loop structure and I be a non empty subset of R. Then $\{0_R\} * I = \{0_R\}$.

(82) Let R be a left zeroed right zeroed add-cancelable distributive non empty double loop structure, I be an add closed right ideal non empty subset of R, and J be an add closed left ideal non empty subset of R. Then $I * J \subseteq I \cap J$.

(83) Let R be an Abelian left zeroed right zeroed add-cancelable add-associative associative distributive non empty double loop structure and I, J, K be right ideal non empty subsets of R. Then $I*(J+K) = I*J+I*K$.

(84) Let R be an Abelian left zeroed right zeroed add-cancelable add-associative commutative associative distributive non empty double loop structure and I, J be right ideal non empty subsets of R. Then $(I + J) * (I \cap J) \subseteq I * J$.

(85) Let R be a right zeroed add-left-cancelable left distributive non empty double loop structure and I, J be add closed left ideal non empty subsets of R. Then $(I + J) * (I \cap J) \subseteq I \cap J$.

Let R be a non empty loop structure and let I, J be subsets of R. We say that I, J are co-prime if and only if:

(Def. 23) $I + J =$ the carrier of R.

We now state two propositions:

(86) Let R be a left zeroed left unital non empty double loop structure and I, J be non empty subsets of R. If I, J are co-prime, then $I \cap J \subseteq (I + J) * (I \cap J)$.

(87) Let R be an Abelian left zeroed right zeroed add-cancelable add-associative left unital commutative associative distributive non empty double loop structure, I be an add closed left ideal right ideal non empty subset of R, and J be an add closed left ideal non empty subset of R. If I, J are co-prime, then $I * J = I \cap J$.

Let R be a non empty groupoid and let I, J be subsets of R. The functor $I \,\%\, J$ yields a subset of R and is defined by:

(Def. 24) $I \,\%\, J = \{a; a$ ranges over elements of R: $a \cdot J \subseteq I\}$.

Let R be a right zeroed add-left-cancelable left distributive non empty double loop structure and let I, J be left ideal non empty subsets of R. One can check that $I \,\%\, J$ is non empty.

Let R be a right zeroed add-left-cancelable left distributive non empty double loop structure and let I, J be add closed left ideal non empty subsets of R. One can check that $I \,\%\, J$ is add closed.

Let R be a right zeroed add-left-cancelable left distributive associative commutative non empty double loop structure and let I, J be left ideal non empty subsets of R. Note that $I \,\%\, J$ is left ideal and $I \,\%\, J$ is right ideal.

We now state several propositions:

(88) Let R be a non empty multiplicative loop structure, I be a right ideal non empty subset of R, and J be a subset of R. Then $I \subseteq I \,\%\, J$.

(89) Let R be a right zeroed add-left-cancelable left distributive non empty double loop structure, I be an add closed left ideal non empty subset of R, and J be a subset of R. Then $(I \,\%\, J) * J \subseteq I$.

(90) Let R be a left zeroed add-right-cancelable right distributive non empty double loop structure, I be an add closed right ideal non empty subset of R, and J be a subset of R. Then $(I \,\%\, J) * J \subseteq I$.

(91) Let R be a left zeroed add-right-cancelable right distributive commutative associative non empty double loop structure, I be an add closed right ideal non empty subset of R, and J, K be subsets of R. Then $(I \,\%\, J) \,\%\, K = I \,\%\, (J * K)$.

(92) For every non empty multiplicative loop structure R and for all subsets I, J, K of R holds $(J \cap K) \,\%\, I = (J \,\%\, I) \cap (K \,\%\, I)$.

(93) Let R be a left zeroed right zeroed add-right-cancelable right distributive non empty double loop structure, I be an add closed subset of R, and J, K

be right ideal non empty subsets of R. Then $I\%(J+K) = (I\%J)\cap(I\%K)$.

Let R be a unital non empty double loop structure and let I be a subset of R. The functor $\sqrt{I}$ yielding a subset of R is defined as follows:

(Def. 25) $\sqrt{I} = \{a; a$ ranges over elements of R: $\bigvee_{n\,:\,\text{natural number}}\ a^n \in I\}$.

Let R be a unital non empty double loop structure and let I be a non empty subset of R. One can verify that $\sqrt{I}$ is non empty.

Let R be an Abelian add-associative left zeroed right zeroed commutative associative add-cancelable distributive unital non empty double loop structure and let I be an add closed right ideal non empty subset of R. Observe that $\sqrt{I}$ is add closed.

Let R be a unital commutative associative non empty double loop structure and let I be a left ideal non empty subset of R. Observe that $\sqrt{I}$ is left ideal and $\sqrt{I}$ is right ideal.

One can prove the following propositions:

(94) Let R be a unital associative non empty double loop structure, I be a non empty subset of R, and a be an element of R. Then $a \in \sqrt{I}$ if and only if there exists a natural number n such that $a^n \in \sqrt{I}$.

(95) Let R be a left zeroed right zeroed add-cancelable distributive unital associative non empty double loop structure, I be an add closed right ideal non empty subset of R, and J be an add closed left ideal non empty subset of R. Then $\sqrt{I * J} = \sqrt{I \cap J}$.

6. Noetherian Rings and PIDs

Let L be a non empty double loop structure and let I be an ideal of L. We say that I is finitely generated if and only if:

(Def. 26) There exists a non empty finite subset F of the carrier of L such that $I = F$–ideal.

Let L be a non empty double loop structure. Observe that there exists an ideal of L which is finitely generated.

Let L be a non empty double loop structure and let F be a non empty finite subset of L. Note that F–ideal is finitely generated.

Let L be a non empty double loop structure. We say that L is Noetherian if and only if:

(Def. 27) Every ideal of L is finitely generated.

Let us observe that there exists a non empty double loop structure which is Euclidian, Abelian, add-associative, right zeroed, right complementable, well unital, distributive, commutative, associative, and non degenerated.

Let L be a non empty double loop structure and let I be an ideal of L. We say that I is principal if and only if:

(Def. 28) There exists an element e of the carrier of L such that $I = \{e\}$–ideal.

Let L be a non empty double loop structure. We say that L is PID if and only if:

(Def. 29) Every ideal of L is principal.

One can prove the following three propositions:

(96) Let L be a non empty double loop structure and F be a non empty subset of the carrier of L. Suppose $F \neq \{0_L\}$. Then there exists an element x of the carrier of L such that $x \neq 0_L$ and $x \in F$.

(97) Every add-associative left zeroed right zeroed right complementable distributive left unital Euclidian non empty double loop structure is PID.

(98) For every non empty double loop structure L such that L is PID holds L is Noetherian.

Let us note that INT.Ring is Noetherian.

Let us observe that there exists a non empty double loop structure which is Noetherian, Abelian, add-associative, right zeroed, right complementable, well unital, distributive, commutative, associative, and non degenerated.

Next we state two propositions:

(99) Let R be a Noetherian add-associative left zeroed right zeroed add-cancelable associative distributive well unital non empty double loop structure and B be a non empty subset of the carrier of R. Then there exists a non empty finite subset C of the carrier of R such that $C \subseteq B$ and C–ideal $= B$–ideal.

(100) Let R be a non empty double loop structure. Suppose that for every non empty subset B of the carrier of R there exists a non empty finite subset C of the carrier of R such that $C \subseteq B$ and C–ideal $= B$–ideal. Let a be a sequence of R. Then there exists a natural number m such that $a(m+1) \in (\mathrm{rng}(a{\restriction}\mathbb{Z}_{m+1}))$–ideal.

Let X, Y be non empty sets, let f be a function from X into Y, and let A be a non empty subset of X. One can check that $f{\restriction}A$ is non empty.

The following two propositions are true:

(101) Let R be a non empty double loop structure. Suppose that for every sequence a of R there exists a natural number m such that $a(m+1) \in (\mathrm{rng}(a{\restriction}\mathbb{Z}_{m+1}))$–ideal. Then there does not exist a function F from $\mathbb{N}$ into $2^{\text{the carrier of } R}$ such that

(i) for every natural number i holds $F(i)$ is an ideal of R, and

(ii) for all natural numbers j, k such that $j < k$ holds $F(j) \subseteq F(k)$ and $F(j) \neq F(k)$.

(102) Let R be a non empty double loop structure. Suppose that it is not true that there exists a function F from $\mathbb{N}$ into $2^{\text{the carrier of } R}$ such that for every natural number i holds $F(i)$ is an ideal of R and for all natural numbers j, k such that $j < k$ holds $F(j) \subseteq F(k)$ and $F(j) \neq F(k)$. Then R is Noetherian.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] Thomas Becker and Volker Weispfenning. *Gröbner bases: A Computational Approach to Commutative Algebra.* Springer-Verlag, New York, Berlin, 1993.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[9] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[10] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[11] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.
[12] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[13] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[14] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[15] Christoph Schwarzweller. The correctness of the generic algorithms of Brown and Henrici concerning addition and multiplication in fraction fields. *Formalized Mathematics*, 6(**3**):381–388, 1997.
[16] Christoph Schwarzweller. The ring of integers, euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[17] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.
[18] Wojciech Skaba and Michał Muzalewski. From double loops to fields. *Formalized Mathematics*, 2(**1**):185–191, 1991.
[19] Dariusz Surowik. Cyclic groups and some of their properties - part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[20] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[21] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[22] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[23] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[24] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[25] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[26] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 20, 2000