

# Characterization and Existence of Gröbner Bases

Christoph Schwarzweller  
University of Tübingen

**Summary.** We continue the Mizar formalization of Gröbner bases following [8]. In this article we prove a number of characterizations of Gröbner bases among them that Gröbner bases are convergent rewriting systems. We also show the existence and uniqueness of reduced Gröbner bases.

MML Identifier: GROEBB\_1.

WWW: [http://mizar.org/JFM/Vol15/groeb\\_1.html](http://mizar.org/JFM/Vol15/groeb_1.html)

The articles [24], [32], [34], [33], [10], [4], [18], [28], [11], [30], [12], [14], [5], [2], [31], [9], [7], [16], [17], [13], [21], [20], [25], [27], [19], [1], [6], [15], [23], [29], [26], [3], and [22] provide the notation and terminology for this paper.

## 1. PRELIMINARIES

Let  $n$  be an ordinal number, let  $L$  be a right zeroed add-associative right complementable unital distributive non trivial double loop structure, and let  $p$  be a polynomial of  $n, L$ . Then  $\{p\}$  is a non empty finite subset of  $\text{Polynom-Ring}(n, L)$ .

We now state several propositions:

- (1) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n, L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $f, p, g$  be polynomials of  $n, L$ . Suppose  $f$  reduces to  $g, p, T$ . Then there exists a monomial  $m$  of  $n, L$  such that  $g = f - m * p$ .
- (2) Let  $n$  be an ordinal number,  $T$  be an admissible connected term order of  $n, L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and  $f, p, g$  be polynomials of  $n, L$ . Suppose  $f$  reduces to  $g, p, T$ . Then there exists a monomial  $m$  of  $n, L$  such that  $g = f - m * p$  and  $\text{HT}(m * p, T) \notin \text{Support } g$  and  $\text{HT}(m * p, T) \leq_T \text{HT}(f, T)$ .
- (3) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n, L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure,  $f, g$  be polynomials of  $n, L$ , and  $P, Q$  be subsets of  $\text{Polynom-Ring}(n, L)$ . If  $P \subseteq Q$ , then if  $f$  reduces to  $g, P, T$ , then  $f$  reduces to  $g, Q, T$ .
- (4) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n, L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $P, Q$  be subsets of  $\text{Polynom-Ring}(n, L)$ . If  $P \subseteq Q$ , then  $\text{PolyRedRel}(P, T) \subseteq \text{PolyRedRel}(Q, T)$ .
- (5) Let  $n$  be an ordinal number,  $L$  be a right zeroed add-associative right complementable non empty double loop structure, and  $p$  be a polynomial of  $n, L$ . Then  $\text{Support}(-p) = \text{Support } p$ .

- (6) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n$ ,  $L$  be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, and  $p$  be a polynomial of  $n$ ,  $L$ . Then  $\text{HT}(-p, T) = \text{HT}(p, T)$ .
- (7) Let  $n$  be an ordinal number,  $T$  be an admissible connected term order of  $n$ ,  $L$  be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, and  $p, q$  be polynomials of  $n$ ,  $L$ . Then  $\text{HT}(p - q, T) \leq_T \max_T(\text{HT}(p, T), \text{HT}(q, T))$ .
- (8) Let  $n$  be an ordinal number,  $T$  be an admissible connected term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $p, q$  be polynomials of  $n$ ,  $L$ . If  $\text{Support } q \subseteq \text{Support } p$ , then  $q \leq_T p$ .
- (9) Let  $n$  be an ordinal number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure, and  $f, p$  be non-zero polynomials of  $n$ ,  $L$ . If  $f$  is reducible wrt  $p, T$ , then  $\text{HT}(p, T) \leq_T \text{HT}(f, T)$ .

## 2. CHARACTERIZATION OF GRÖBNER BASES

The following propositions are true:

- (10) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non trivial double loop structure, and  $p$  be a polynomial of  $n$ ,  $L$ . Then  $\text{PolyRedRel}(\{p\}, T)$  is locally-confluent.
- (11) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure, and  $P$  be a subset of  $\text{Polynom-Ring}(n, L)$ . Given a polynomial  $p$  of  $n$ ,  $L$  such that  $p \in P$  and  $P$ -ideal =  $\{p\}$ -ideal. Then  $\text{PolyRedRel}(P, T)$  is locally-confluent.

Let  $n$  be an ordinal number, let  $T$  be a connected term order of  $n$ , let  $L$  be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, and let  $P$  be a subset of  $\text{Polynom-Ring}(n, L)$ . The functor  $\text{HT}(P, T)$  yielding a subset of  $\text{Bags } n$  is defined as follows:

(Def. 1)  $\text{HT}(P, T) = \{\text{HT}(p, T); p \text{ ranges over polynomials of } n, L: p \in P \wedge p \neq 0_n L\}$ .

Let  $n$  be an ordinal number and let  $S$  be a subset of  $\text{Bags } n$ . The functor  $\text{multiples}(S)$  yields a subset of  $\text{Bags } n$  and is defined as follows:

(Def. 2)  $\text{multiples}(S) = \{b; b \text{ ranges over elements of } \text{Bags } n : \bigvee_{b': \text{bag of } n} (b' \in S \wedge b' \mid b)\}$ .

The following propositions are true:

- (12) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and  $P$  be a subset of  $\text{Polynom-Ring}(n, L)$ . If  $\text{PolyRedRel}(P, T)$  is locally-confluent, then  $\text{PolyRedRel}(P, T)$  is confluent.
- (13) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $P$  be a subset of  $\text{Polynom-Ring}(n, L)$ . If  $\text{PolyRedRel}(P, T)$  is confluent, then  $\text{PolyRedRel}(P, T)$  has unique normal form property.

- (14) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and  $P$  be a subset of Polynom-Ring( $n, L$ ). Suppose PolyRedRel( $P, T$ ) has unique normal form property. Then PolyRedRel( $P, T$ ) has Church-Rosser property.
- (15) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and  $P$  be a non empty subset of Polynom-Ring( $n, L$ ). Suppose PolyRedRel( $P, T$ ) has Church-Rosser property. Let  $f$  be a polynomial of  $n, L$ . If  $f \in P$ -ideal, then PolyRedRel( $P, T$ ) reduces  $f$  to  $0_n L$ .
- (16) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $P$  be a subset of Polynom-Ring( $n, L$ ). Suppose that for every polynomial  $f$  of  $n, L$  such that  $f \in P$ -ideal holds PolyRedRel( $P, T$ ) reduces  $f$  to  $0_n L$ . Let  $f$  be a non-zero polynomial of  $n, L$ . If  $f \in P$ -ideal, then  $f$  is reducible wrt  $P, T$ .
- (17) Let  $n$  be a natural number,  $T$  be an admissible connected term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and  $P$  be a subset of Polynom-Ring( $n, L$ ). Suppose that for every non-zero polynomial  $f$  of  $n, L$  such that  $f \in P$ -ideal holds  $f$  is reducible wrt  $P, T$ . Let  $f$  be a non-zero polynomial of  $n, L$ . If  $f \in P$ -ideal, then  $f$  is top reducible wrt  $P, T$ .
- (18) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $P$  be a subset of Polynom-Ring( $n, L$ ). Suppose that for every non-zero polynomial  $f$  of  $n, L$  such that  $f \in P$ -ideal holds  $f$  is top reducible wrt  $P, T$ . Let  $b$  be a bag of  $n$ . If  $b \in \text{HT}(P\text{-ideal}, T)$ , then there exists a bag  $b'$  of  $n$  such that  $b' \in \text{HT}(P, T)$  and  $b' \mid b$ .
- (19) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $P$  be a subset of Polynom-Ring( $n, L$ ). Suppose that for every bag  $b$  of  $n$  such that  $b \in \text{HT}(P\text{-ideal}, T)$  there exists a bag  $b'$  of  $n$  such that  $b' \in \text{HT}(P, T)$  and  $b' \mid b$ . Then  $\text{HT}(P\text{-ideal}, T) \subseteq \text{multiples}(\text{HT}(P, T))$ .
- (20) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure, and  $P$  be a subset of Polynom-Ring( $n, L$ ). If  $\text{HT}(P\text{-ideal}, T) \subseteq \text{multiples}(\text{HT}(P, T))$ , then PolyRedRel( $P, T$ ) is locally-confluent.

Let  $n$  be an ordinal number, let  $T$  be a connected term order of  $n$ , let  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and let  $G$  be a subset of Polynom-Ring( $n, L$ ). We say that  $G$  is a Groebner basis wrt  $T$  if and only if:

(Def. 3) PolyRedRel( $G, T$ ) is locally-confluent.

Let  $n$  be an ordinal number, let  $T$  be a connected term order of  $n$ , let  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and let  $G, I$  be subsets of Polynom-Ring( $n, L$ ). We say that  $G$  is a Groebner basis of  $I, T$  if and only if:

(Def. 4)  $G$ -ideal =  $I$  and PolyRedRel( $G, T$ ) is locally-confluent.

The following propositions are true:

- (21) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure, and  $G, P$  be non empty subsets of Polynom-Ring( $n, L$ ). If  $G$  is a Groebner basis of  $P, T$ , then PolyRedRel( $G, T$ ) is a completion of PolyRedRel( $P, T$ ).
- (22) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure,  $p, q$  be elements of Polynom-Ring( $n, L$ ), and  $G$  be a non empty subset of Polynom-Ring( $n, L$ ). Suppose  $G$  is a Groebner basis wrt  $T$ . Then  $p \equiv q \pmod{G\text{-ideal}}$  if and only if  $\text{nf}_{\text{PolyRedRel}(G, T)}(p) = \text{nf}_{\text{PolyRedRel}(G, T)}(q)$ .
- (23) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure,  $f$  be a polynomial of  $n, L$ , and  $P$  be a non empty subset of Polynom-Ring( $n, L$ ). Suppose  $P$  is a Groebner basis wrt  $T$ . Then  $f \in P\text{-ideal}$  if and only if PolyRedRel( $P, T$ ) reduces  $f$  to  $0_n L$ .
- (24) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure,  $I$  be a subset of Polynom-Ring( $n, L$ ), and  $G$  be a non empty subset of Polynom-Ring( $n, L$ ). Suppose  $G$  is a Groebner basis of  $I, T$ . Let  $f$  be a polynomial of  $n, L$ . If  $f \in I$ , then PolyRedRel( $G, T$ ) reduces  $f$  to  $0_n L$ .
- (25) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n, L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $G, I$  be subsets of Polynom-Ring( $n, L$ ). Suppose that for every polynomial  $f$  of  $n, L$  such that  $f \in I$  holds PolyRedRel( $G, T$ ) reduces  $f$  to  $0_n L$ . Let  $f$  be a non-zero polynomial of  $n, L$ . If  $f \in I$ , then  $f$  is reducible wrt  $G, T$ .
- (26) Let  $n$  be a natural number,  $T$  be an admissible connected term order of  $n, L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure,  $I$  be an add closed left ideal subset of Polynom-Ring( $n, L$ ), and  $G$  be a subset of Polynom-Ring( $n, L$ ). Suppose  $G \subseteq I$ . Suppose that for every non-zero polynomial  $f$  of  $n, L$  such that  $f \in I$  holds  $f$  is reducible wrt  $G, T$ . Let  $f$  be a non-zero polynomial of  $n, L$ . If  $f \in I$ , then  $f$  is top reducible wrt  $G, T$ .
- (27) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n, L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $G, I$  be subsets of Polynom-Ring( $n, L$ ). Suppose that for every non-zero polynomial  $f$  of  $n, L$  such that  $f \in I$  holds  $f$  is top reducible wrt  $G, T$ . Let  $b$  be a bag of  $n$ . If  $b \in \text{HT}(I, T)$ , then there exists a bag  $b'$  of  $n$  such that  $b' \in \text{HT}(G, T)$  and  $b' \mid b$ .
- (28) Let  $n$  be an ordinal number,  $T$  be a connected term order of  $n, L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and  $G, I$  be subsets of Polynom-Ring( $n, L$ ). Suppose that for every bag  $b$  of  $n$  such that  $b \in \text{HT}(I, T)$  there exists a bag  $b'$  of  $n$  such that  $b' \in \text{HT}(G, T)$  and  $b' \mid b$ . Then  $\text{HT}(I, T) \subseteq \text{multiples}(\text{HT}(G, T))$ .
- (29) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n, L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure,  $I$  be an add closed left ideal non empty subset of Polynom-Ring( $n, L$ ), and  $G$  be a non empty subset of Polynom-Ring( $n, L$ ). If  $G \subseteq I$ , then if  $\text{HT}(I, T) \subseteq \text{multiples}(\text{HT}(G, T))$ , then  $G$  is a Groebner basis of  $I, T$ .

## 3. EXISTENCE OF GRÖBNER BASES

The following four propositions are true:

- (30) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ , and  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non trivial double loop structure. Then  $\{0_nL\}$  is a Groebner basis of  $\{0_nL\}, T$ .
- (31) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non trivial double loop structure, and  $p$  be a polynomial of  $n, L$ . Then  $\{p\}$  is a Groebner basis of  $\{p\}$ -ideal,  $T$ .
- (32) Let  $T$  be an admissible connected term order of  $\emptyset$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure,  $I$  be an add closed left ideal non empty subset of Polynom-Ring( $\emptyset, L$ ), and  $P$  be a non empty subset of Polynom-Ring( $\emptyset, L$ ). If  $P \subseteq I$  and  $P \neq \{0_\emptyset L\}$ , then  $P$  is a Groebner basis of  $I, T$ .
- (33) Let  $n$  be a non empty ordinal number,  $T$  be an admissible connected term order of  $n$ , and  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure. Then there exists a subset  $P$  of Polynom-Ring( $n, L$ ) such that  $P$  is not a Groebner basis wrt  $T$ .

Let  $n$  be an ordinal number. The functor DivOrder( $n$ ) yields an order in Bags $n$  and is defined by:

- (Def. 5) For all bags  $b_1, b_2$  of  $n$  holds  $\langle b_1, b_2 \rangle \in \text{DivOrder}(n)$  iff  $b_1 | b_2$ .

Let  $n$  be a natural number. Observe that  $\langle \text{Bags}n, \text{DivOrder}(n) \rangle$  is Dickson.

The following three propositions are true:

- (34) For every natural number  $n$  and for every subset  $N$  of  $\langle \text{Bags}n, \text{DivOrder}(n) \rangle$  holds there exists a finite subset of Bags $n$  which is Dickson basis of  $N, \langle \text{Bags}n, \text{DivOrder}(n) \rangle$ .
- (35) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure, and  $I$  be an add closed left ideal non empty subset of Polynom-Ring( $n, L$ ). Then there exists a finite subset of Polynom-Ring( $n, L$ ) which is a Groebner basis of  $I, T$ .
- (36) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure, and  $I$  be an add closed left ideal non empty subset of Polynom-Ring( $n, L$ ). Suppose  $I \neq \{0_nL\}$ . Then there exists a finite subset  $G$  of Polynom-Ring( $n, L$ ) such that  $G$  is a Groebner basis of  $I, T$  and  $0_nL \notin G$ .

Let  $n$  be an ordinal number, let  $T$  be a connected term order of  $n$ , let  $L$  be a non empty multiplicative loop with zero structure, and let  $p$  be a polynomial of  $n, L$ . We say that  $p$  is monic wrt  $T$  if and only if:

- (Def. 6)  $\text{HC}(p, T) = \mathbf{1}_L$ .

Let  $n$  be an ordinal number, let  $T$  be a connected term order of  $n$ , let  $L$  be a right zeroed add-associative right complementable commutative associative well unital distributive field-like non trivial non empty double loop structure, and let  $P$  be a subset of Polynom-Ring( $n, L$ ). We say that  $P$  is reduced wrt  $T$  if and only if:

- (Def. 7) For every polynomial  $p$  of  $n, L$  such that  $p \in P$  holds  $p$  is monic wrt  $T$  and irreducible wrt  $P \setminus \{p\}, T$ .

We introduce  $P$  is autoreduced wrt  $T$  as a synonym of  $P$  is reduced wrt  $T$ .

One can prove the following propositions:

- (37) Let  $n$  be an ordinal number,  $T$  be an admissible connected term order of  $n$ ,  $L$  be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure,  $I$  be an add closed left ideal subset of Polynom-Ring( $n, L$ ),  $m$  be a monomial of  $n, L$ , and  $f, g$  be polynomials of  $n, L$ . Suppose  $f \in I$  and  $g \in I$  and  $\text{HM}(f, T) = m$  and  $\text{HM}(g, T) = m$ . Suppose that
  - (i) it is not true that there exists a polynomial  $p$  of  $n, L$  such that  $p \in I$  and  $p <_T f$  and  $\text{HM}(p, T) = m$ , and
  - (ii) it is not true that there exists a polynomial  $p$  of  $n, L$  such that  $p \in I$  and  $p <_T g$  and  $\text{HM}(p, T) = m$ .
 Then  $f = g$ .
- (38) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure,  $I$  be an add closed left ideal non empty subset of Polynom-Ring( $n, L$ ),  $G$  be a subset of Polynom-Ring( $n, L$ ),  $p$  be a polynomial of  $n, L$ , and  $q$  be a non-zero polynomial of  $n, L$ . Suppose  $p \in G$  and  $q \in G$  and  $p \neq q$  and  $\text{HT}(q, T) \mid \text{HT}(p, T)$ . If  $G$  is a Groebner basis of  $I, T$ , then  $G \setminus \{p\}$  is a Groebner basis of  $I, T$ .
- (39) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure, and  $I$  be an add closed left ideal non empty subset of Polynom-Ring( $n, L$ ). If  $I \neq \{0_n L\}$ , then there exists a finite subset  $G$  of Polynom-Ring( $n, L$ ) which is a Groebner basis of  $I, T$  and reduced wrt  $T$ .
- (40) Let  $n$  be a natural number,  $T$  be a connected admissible term order of  $n$ ,  $L$  be an Abelian add-associative right complementable right zeroed commutative associative well unital distributive field-like non degenerated non empty double loop structure,  $I$  be an add closed left ideal non empty subset of Polynom-Ring( $n, L$ ), and  $G_1, G_2$  be non empty finite subsets of Polynom-Ring( $n, L$ ). Suppose  $G_1$  is a Groebner basis of  $I, T$  and reduced wrt  $T$  and  $G_2$  is a Groebner basis of  $I, T$  and reduced wrt  $T$ . Then  $G_1 = G_2$ .

## REFERENCES

- [1] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Journal of Formalized Mathematics*, 12, 2000. [http://mizar.org/JFM/Vol12/ideal\\_1.html](http://mizar.org/JFM/Vol12/ideal_1.html).
- [2] Grzegorz Bancerek. Cardinal numbers. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/card\\_1.html](http://mizar.org/JFM/Vol1/card_1.html).
- [3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/nat\\_1.html](http://mizar.org/JFM/Vol1/nat_1.html).
- [4] Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. <http://mizar.org/JFM/Vol1/ordinal1.html>.
- [5] Grzegorz Bancerek. König's theorem. *Journal of Formalized Mathematics*, 2, 1990. [http://mizar.org/JFM/Vol2/card\\_3.html](http://mizar.org/JFM/Vol2/card_3.html).
- [6] Grzegorz Bancerek. Reduction relations. *Journal of Formalized Mathematics*, 7, 1995. <http://mizar.org/JFM/Vol7/rewrite1.html>.
- [7] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/finseq\\_1.html](http://mizar.org/JFM/Vol1/finseq_1.html).
- [8] Thomas Becker and Volker Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra*. Springer-Verlag, New York, Berlin, 1993.
- [9] Józef Białas. Group and field definitions. *Journal of Formalized Mathematics*, 1, 1989. <http://mizar.org/JFM/Vol1/realset1.html>.
- [10] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/funct\\_1.html](http://mizar.org/JFM/Vol1/funct_1.html).
- [11] Czesław Byliński. Partial functions. *Journal of Formalized Mathematics*, 1, 1989. <http://mizar.org/JFM/Vol1/partfun1.html>.

- [12] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/finset\\_1.html](http://mizar.org/JFM/Vol1/finset_1.html).
- [13] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/vectsp\\_1.html](http://mizar.org/JFM/Vol1/vectsp_1.html).
- [14] Gilbert Lee and Piotr Rudnicki. Dickson's lemma. *Journal of Formalized Mathematics*, 14, 2002. <http://mizar.org/JFM/Vol14/dickson.html>.
- [15] Gilbert Lee and Piotr Rudnicki. On ordering of bags. *Journal of Formalized Mathematics*, 14, 2002. <http://mizar.org/JFM/Vol14/bagorder.html>.
- [16] Beata Madras. Product of family of universal algebras. *Journal of Formalized Mathematics*, 5, 1993. [http://mizar.org/JFM/Vol5/pralg\\_1.html](http://mizar.org/JFM/Vol5/pralg_1.html).
- [17] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. [http://mizar.org/JFM/Vol2/vectsp\\_2.html](http://mizar.org/JFM/Vol2/vectsp_2.html).
- [18] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Journal of Formalized Mathematics*, 2, 1990. [http://mizar.org/JFM/Vol2/algstr\\_1.html](http://mizar.org/JFM/Vol2/algstr_1.html).
- [19] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Journal of Formalized Mathematics*, 11, 1999. <http://mizar.org/JFM/Vol11/polynom1.html>.
- [20] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Journal of Formalized Mathematics*, 12, 2000. <http://mizar.org/JFM/Vol12/binom.html>.
- [21] Christoph Schwarzweller. More on multivariate polynomials: Monomials and constant polynomials. *Journal of Formalized Mathematics*, 13, 2001. <http://mizar.org/JFM/Vol13/polynom7.html>.
- [22] Christoph Schwarzweller. Polynomial reduction. *Journal of Formalized Mathematics*, 14, 2002. <http://mizar.org/JFM/Vol14/polyred.html>.
- [23] Christoph Schwarzweller. Term orders. *Journal of Formalized Mathematics*, 14, 2002. <http://mizar.org/JFM/Vol14/termord.html>.
- [24] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. <http://mizar.org/JFM/Axiomatics/tarski.html>.
- [25] Andrzej Trybulec. Many-sorted sets. *Journal of Formalized Mathematics*, 5, 1993. <http://mizar.org/JFM/Vol5/pboole.html>.
- [26] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. <http://mizar.org/JFM/Addenda/numbers.html>.
- [27] Wojciech A. Trybulec. Partially ordered sets. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/orders\\_1.html](http://mizar.org/JFM/Vol1/orders_1.html).
- [28] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/rvect\\_1.html](http://mizar.org/JFM/Vol1/rvect_1.html).
- [29] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. [http://mizar.org/JFM/Vol2/group\\_1.html](http://mizar.org/JFM/Vol2/group_1.html).
- [30] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. [http://mizar.org/JFM/Vol2/finseq\\_4.html](http://mizar.org/JFM/Vol2/finseq_4.html).
- [31] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/subset\\_1.html](http://mizar.org/JFM/Vol1/subset_1.html).
- [32] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/relat\\_1.html](http://mizar.org/JFM/Vol1/relat_1.html).
- [33] Edmund Woronowicz. Relations defined on sets. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/reiset\\_1.html](http://mizar.org/JFM/Vol1/reiset_1.html).
- [34] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Journal of Formalized Mathematics*, 1, 1989. [http://mizar.org/JFM/Vol1/relat\\_2.html](http://mizar.org/JFM/Vol1/relat_2.html).

Received June 11, 2003

Published January 2, 2004

---