FORMALIZED MATHEMATICS
Volume 11, Number 3, 2003
University of Białystok

# 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: GROEB_1.

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


© 2003 University of Białystok
ISSN 1426–2630

$f$ reduces to $g$, $p$, $T$. Then there exists a monomial $m$ of $n$, $L$ such that $g = f - m*p$ and $\mathrm{HT}(m*p, T) \notin \operatorname{Support} g$ and $\mathrm{HT}(m*p, T) \preccurlyeq_T \mathrm{HT}(f, T)$.

(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 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 Polynom-Ring$(n, L)$. If $P \subseteq Q$, then $\mathrm{PolyRedRel}(P, T) \subseteq \mathrm{PolyRedRel}(Q, T)$.

(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 $\operatorname{Support}(-p) = \operatorname{Support} p$.

(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 $\mathrm{HT}(-p, T) = \mathrm{HT}(p, T)$.

(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 $\mathrm{HT}(p - q, T) \preccurlyeq_T \max_T(\mathrm{HT}(p, T), \mathrm{HT}(q, T))$.

(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 $\operatorname{Support} q \subseteq \operatorname{Support} p$, then $q \preccurlyeq_T p$.

(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 $\mathrm{HT}(p, T) \preccurlyeq_T \mathrm{HT}(f, T)$.

## 2. Characterization of Gröbner Bases

Next we state two propositions:

(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 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 Polynom-Ring$(n, L)$. Given a polynomial $p$ of $n$, $L$ such that $p \in P$ and $P$–ideal $= \{p\}$–ideal. 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 a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, and let $P$ be a subset of Polynom-Ring$(n, L)$. The functor HT$(P, T)$ yields a subset of Bags $n$ and is defined as follows:

(Def. 1) HT$(P, T) = \{\mathrm{HT}(p, T); p$ 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 Bags $n$. The functor multiples$(S)$ yields a subset of Bags $n$ and is defined by:

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

We now state several propositions:

(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 Polynom-Ring$(n, L)$. If PolyRedRel$(P, T)$ is locally-confluent, then 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 Polynom-Ring$(n, L)$. If PolyRedRel$(P, T)$ is confluent, then 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 $b \in \mathrm{HT}(P\text{–ideal}, T)$, then there exists a bag $b'$ of $n$ such that $b' \in \mathrm{HT}(P, T)$ 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 $b \in \mathrm{HT}(P\text{–ideal}, T)$ there exists a bag $b'$ of $n$ such that $b' \in \mathrm{HT}(P, T)$ and $b' \mid b$. Then $\mathrm{HT}(P\text{–ideal}, T) \subseteq$ multiples$(\mathrm{HT}(P, T))$.

(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 $\mathrm{HT}(P\text{–ideal}, T) \subseteq$ multiples$(\mathrm{HT}(P, T))$, 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.

One can prove the following propositions:

(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 $p \equiv q (\mathrm{mod}\, G\text{–ideal})$ if and only if $\mathrm{nf}_{\mathrm{PolyRedRel}(G,T)}(p) = \mathrm{nf}_{\mathrm{PolyRedRel}(G,T)}(q)$.

(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 $f \in P$–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 $b \in \mathrm{HT}(I, T)$, then there exists a bag $b'$ of $n$ such that $b' \in \mathrm{HT}(G, T)$ 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 $b \in \mathrm{HT}(I, T)$ there exists a bag $b'$ of $n$ such that $b' \in \mathrm{HT}(G, T)$ and $b' \mid b$. Then $\mathrm{HT}(I, T) \subseteq \mathrm{multiples}(\mathrm{HT}(G, T))$.

(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 $\mathrm{HT}(I, T) \subseteq \mathrm{multiples}(\mathrm{HT}(G, T))$, then $G$ is a Groebner basis of $I$, $T$.

## 3. Existence of Gröbner Bases

Next we state four propositions:

(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 $\{0_n L\}$ is a Groebner basis of $\{0_n L\}$, $T$.

(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 $\langle b_1, b_2 \rangle \in \mathrm{DivOrder}(n)$ iff $b_1 \mid b_2$.

Let $n$ be a natural number. One can check that $\langle \mathrm{Bags}\, n, \mathrm{DivOrder}(n) \rangle$ is Dickson.

The following propositions are true:

(34) For every natural number $n$ and for every subset $N$ of the carrier of $\langle \mathrm{Bags}\, n, \mathrm{DivOrder}(n) \rangle$ holds there exists a finite subset of Bags $n$ which is Dickson basis of $N$, $\langle \mathrm{Bags}\, n, \mathrm{DivOrder}(n) \rangle$.

(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 $I \neq \{0_n L\}$. Then there exists a finite subset $G$ of Polynom-Ring$(n, L)$ such that $G$ is a Groebner basis of $I$, $T$ and $0_n L \notin G$.

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) $\mathrm{HC}(p, T) = \mathbf{1}_L$.

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 $T$.

Next we state four 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 $\mathrm{HM}(f, T) = m$ and $\mathrm{HM}(g, T) = m$. 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 $\mathrm{HM}(p, T) = m$, 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 $\mathrm{HM}(p, T) = m$.

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 $\mathrm{HT}(q, T) \mid \mathrm{HT}(p, T)$. 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. *Formalized Mathematics*, 9(**3**):565–582, 2001.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

[5] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[6] Grzegorz Bancerek. Reduction relations. *Formalized Mathematics*, 5(**4**):469–478, 1996.

[7] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[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. *Formalized Mathematics*, 1(**3**):433–439, 1990.

[10] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

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

[13] Gilbert Lee and Piotr Rudnicki. Dickson's lemma. *Formalized Mathematics*, 10(**1**):29–37, 2002.

[14] Gilbert Lee and Piotr Rudnicki. On ordering of bags. *Formalized Mathematics*, 10(**1**):39–46, 2002.

[15] Beata Madras. Product of family of universal algebras. *Formalized Mathematics*, 4(**1**):103–108, 1993.

[16] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.

[17] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.

[18] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.

[19] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

[20] Christoph Schwarzweller. More on multivariate polynomials: Monomials and constant polynomials. *Formalized Mathematics*, 9(**4**):849–855, 2001.

[21] Christoph Schwarzweller. Polynomial reduction. *Formalized Mathematics*, 11(**1**):113–123, 2003.

[22] Christoph Schwarzweller. Term orders. *Formalized Mathematics*, 11(**1**):105–111, 2003.

[23] Andrzej Trybulec. Introduction to arithmetics. *To appear in Formalized Mathematics*.

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

[25] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

[26] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[27] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.

[28] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[29] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

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

[31] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

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

[33] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

*Received June 11, 2003*