JOURNAL OF FORMALIZED MATHEMATICS
Volume 12, Released 2000, Published 2003
Inst. of Computer Science, Univ. of Białystok

The Binomial Theorem for Algebraic Structures[1]

Christoph Schwarzweller
University of Tübingen

Summary. In this paper we prove the well-known binomial theorem for algebraic structures. In doing so we tried to be as modest as possible concerning the algebraic properties of the underlying structure. Consequently, we proved the binomial theorem for "commutative rings" in which the existence of an inverse with respect to addition is replaced by a weaker property of cancellation.

MML Identifier: `BINOM`.

WWW: `http://mizar.org/JFM/Vol12/binom.html`

The articles [12], [6], [17], [13], [2], [4], [5], [1], [16], [18], [3], [10], [7], [8], [15], [9], [14], and [11] provide the notation and terminology for this paper.

1. Preliminaries

Let L be a non empty loop structure. We say that L is add-cancelable if and only if:

(Def. 3)[1] For all elements a, b, c of L holds if $a+b=a+c$, then $b=c$ and if $b+a=c+a$, then $b=c$.

One can verify the following observations:

* there exists a non empty loop structure which is add-left-cancelable,
* there exists a non empty loop structure which is add-right-cancelable, and
* there exists a non empty loop structure which is add-cancelable.

Let us note that every non empty loop structure which is add-left-cancelable and add-right-cancelable is also add-cancelable and every non empty loop structure which is add-cancelable is also add-left-cancelable and add-right-cancelable.

Let us note that every non empty loop structure which is Abelian and add-right-cancelable is also add-left-cancelable and every non empty loop structure which is Abelian and add-left-cancelable is also add-right-cancelable.

Let us mention that every non empty loop structure which is right zeroed, right complementable, and add-associative is also add-right-cancelable.

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

Next we state two propositions:

(1) Let R be a right zeroed add-left-cancelable left distributive non empty double loop structure and a be an element of R. Then $0_R \cdot a = 0_R$.

[1]This work has been partially supported by CALCULEMUS grant HPRN-CT-2000-00102.

[1] The definitions (Def. 1) and (Def. 2) have been removed.

(2) Let R be a left zeroed add-right-cancelable right distributive non empty double loop structure and a be an element of R. Then $a \cdot 0_R = 0_R$.

In this article we present several logical schemes. The scheme *Ind2* deals with a natural number $\mathcal{A}$ and a unary predicate $\mathcal{P}$, and states that:

For every natural number i such that $\mathcal{A} \leq i$ holds $\mathcal{P}[i]$

provided the parameters have the following properties:

- $\mathcal{P}[\mathcal{A}]$, and
- For every natural number j such that $\mathcal{A} \leq j$ holds if $\mathcal{P}[j]$, then $\mathcal{P}[j+1]$.

The scheme *RecDef1* deals with non empty sets $\mathcal{A}$, $\mathcal{B}$, an element $\mathcal{C}$ of $\mathcal{B}$, and a function $\mathcal{D}$ from $[:\mathcal{A}, \mathcal{B}:]$ into $\mathcal{B}$, and states that:

There exists a function g from $[:\mathbb{N}, \mathcal{A}:]$ into $\mathcal{B}$ such that for every element a of $\mathcal{A}$ holds

$g(0, a) = \mathcal{C}$ and for every natural number n holds $g(n+1, a) = \mathcal{D}(a, g(n, a))$

for all values of the parameters.

The scheme *RecDef2* deals with non empty sets $\mathcal{A}$, $\mathcal{B}$, an element $\mathcal{C}$ of $\mathcal{B}$, and a function $\mathcal{D}$ from $[:\mathcal{B}, \mathcal{A}:]$ into $\mathcal{B}$, and states that:

There exists a function g from $[:\mathcal{A}, \mathbb{N}:]$ into $\mathcal{B}$ such that for every element a of $\mathcal{A}$ holds

$g(a, 0) = \mathcal{C}$ and for every natural number n holds $g(a, n+1) = \mathcal{D}(g(a, n), a)$

for all values of the parameters.

2. On Finite Sequences

We now state four propositions:

(3) For every left zeroed non empty loop structure L and for every element a of L holds $\sum\langle a\rangle = a$.

(4) Let R be a left zeroed add-right-cancelable right distributive non empty double loop structure, a be an element of R, and p be a finite sequence of elements of the carrier of R. Then $\sum(a \cdot p) = a \cdot \sum p$.

(5) Let R be a right zeroed add-left-cancelable left distributive non empty double loop structure, a be an element of R, and p be a finite sequence of elements of the carrier of R. Then $\sum(p \cdot a) = \sum p \cdot a$.

(6) Let R be a commutative non empty double loop structure, a be an element of R, and p be a finite sequence of elements of the carrier of R. Then $\sum(p \cdot a) = \sum(a \cdot p)$.

Let R be a non empty loop structure and let p, q be finite sequences of elements of the carrier of R. Let us assume that $\operatorname{dom} p = \operatorname{dom} q$. The functor $p+q$ yielding a finite sequence of elements of the carrier of R is defined by:

(Def. 4) $\operatorname{dom}(p+q) = \operatorname{dom} p$ and for every natural number i such that $1 \leq i$ and $i \leq \operatorname{len}(p+q)$ holds $(p+q)_i = p_i + q_i$.

We now state the proposition

(7) Let R be an Abelian right zeroed add-associative non empty loop structure and p, q be finite sequences of elements of the carrier of R. If $\operatorname{dom} p = \operatorname{dom} q$, then $\sum(p+q) = \sum p + \sum q$.

3. On Powers in Rings

Let R be a unital non empty groupoid, let a be an element of R, and let n be a natural number. The functor a^n yields an element of R and is defined by:

(Def. 5) $a^n = \operatorname{power}_R(a, n)$.

One can prove the following propositions:

(8) For every unital non empty groupoid R and for every element a of R holds $a^0 = 1_R$ and $a^1 = a$.

(9) For every unital non empty groupoid R and for every element a of R and for every natural number n holds $a^{n+1} = a^n \cdot a$.

(10) Let R be a unital associative commutative non empty groupoid, a, b be elements of R, and n be a natural number. Then $(a \cdot b)^n = a^n \cdot b^n$.

(11) Let R be a unital associative non empty groupoid, a be an element of R, and n, m be natural numbers. Then $a^{n+m} = a^n \cdot a^m$.

(12) Let R be a unital associative non empty groupoid, a be an element of R, and n, m be natural numbers. Then $(a^n)^m = a^{n \cdot m}$.

4. On Natural Products in Rings

Let R be a non empty loop structure. The functor Nat-mult-left$R$ yields a function from $[:\mathbb{N}$, the carrier of $R:]$ into the carrier of R and is defined as follows:

(Def. 6) For every element a of R holds $(\text{Nat-mult-left}R)(0, a) = 0_R$ and for every natural number n holds $(\text{Nat-mult-left}R)(n+1, a) = a + (\text{Nat-mult-left}R)(n, a)$.

The functor Nat-mult-right$R$ yielding a function from $[:$the carrier of R, $\mathbb{N}:]$ into the carrier of R is defined as follows:

(Def. 7) For every element a of R holds $(\text{Nat-mult-right}R)(a, 0) = 0_R$ and for every natural number n holds $(\text{Nat-mult-right}R)(a, n+1) = (\text{Nat-mult-right}R)(a, n) + a$.

Let R be a non empty loop structure, let a be an element of R, and let n be a natural number. The functor $n \cdot a$ yields an element of R and is defined as follows:

(Def. 8) $n \cdot a = (\text{Nat-mult-left}R)(n, a)$.

The functor $a \cdot n$ yielding an element of R is defined as follows:

(Def. 9) $a \cdot n = (\text{Nat-mult-right}R)(a, n)$.

One can prove the following propositions:

(13) For every non empty loop structure R and for every element a of R holds $0 \cdot a = 0_R$ and $a \cdot 0 = 0_R$.

(14) For every right zeroed non empty loop structure R and for every element a of R holds $1 \cdot a = a$.

(15) For every left zeroed non empty loop structure R and for every element a of R holds $a \cdot 1 = a$.

(16) Let R be a left zeroed add-associative non empty loop structure, a be an element of R, and n, m be natural numbers. Then $(n+m) \cdot a = n \cdot a + m \cdot a$.

(17) Let R be a right zeroed add-associative non empty loop structure, a be an element of R, and n, m be natural numbers. Then $a \cdot (n+m) = a \cdot n + a \cdot m$.

(18) Let R be a left zeroed right zeroed add-associative non empty loop structure, a be an element of R, and n be a natural number. Then $n \cdot a = a \cdot n$.

(19) Let R be an Abelian non empty loop structure, a be an element of R, and n be a natural number. Then $n \cdot a = a \cdot n$.

(20) Let R be a left zeroed right zeroed add-left-cancelable add-associative left distributive non empty double loop structure, a, b be elements of R, and n be a natural number. Then $(n \cdot a) \cdot b = n \cdot (a \cdot b)$.

(21) Let R be a left zeroed right zeroed add-right-cancelable add-associative distributive non empty double loop structure, a, b be elements of R, and n be a natural number. Then $b \cdot (n \cdot a) = (b \cdot a) \cdot n$.

(22) Let R be a left zeroed right zeroed add-associative add-cancelable distributive non empty double loop structure, a, b be elements of R, and n be a natural number. Then $(a \cdot n) \cdot b = a \cdot (n \cdot b)$.

5. The Binomial Theorem

Let k, n be natural numbers. Then $\binom{n}{k}$ is a natural number.

Let R be a unital non empty double loop structure, let a, b be elements of R, and let n be a natural number. The functor $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle$ yields a finite sequence of elements of the carrier of R and is defined by the conditions (Def. 10).

(Def. 10)(i) $\mathrm{len} \langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle = n + 1$, and

(ii) for all natural numbers i, l, m such that $i \in \mathrm{dom} \langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle$ and $m = i - 1$ and $l = n - m$ holds $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle_i = \binom{n}{m} \cdot a^l \cdot b^m$.

Next we state four propositions:

(23) For every right zeroed unital non empty double loop structure R and for all elements a, b of R holds $\langle \binom{0}{0} a^0 b^0, \ldots, \binom{0}{0} a^0 b^0 \rangle = \langle 1_R \rangle$.

(24) Let R be a right zeroed unital non empty double loop structure, a, b be elements of R, and n be a natural number. Then $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle(1) = a^n$.

(25) Let R be a right zeroed unital non empty double loop structure, a, b be elements of R, and n be a natural number. Then $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle(n+1) = b^n$.

(26) Let R be an Abelian add-associative left zeroed right zeroed commutative associative add-cancelable distributive unital non empty double loop structure, a, b be elements of R, and n be a natural number. Then $(a+b)^n = \sum \langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/nat_1.html`.

[2] 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`.

[3] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/binop_1.html`.

[4] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_1.html`.

[5] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_2.html`.

[6] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/zfmisc_1.html`.

[7] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseq_2.html`.

[8] 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`.

[9] Rafał Kwiatek. Factorial and Newton coefficients. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/newton.html`.

[10] 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`.

[11] 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`.

[12] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. `http://mizar.org/JFM/Axiomatics/tarski.html`.

[13] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. `http://mizar.org/JFM/Addenda/numbers.html`.

[14] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/rlvect_1.html`.

[15] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/group_1.html`.

[16] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseq_4.html`.

[17] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/subset_1.html`.

[18] Edmund Woronowicz. Relations defined on sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relset_1.html`.

Received November 20, 2000

Published January 2, 2004