FORMALIZED MATHEMATICS
Volume 9, Number 3, 2001
University 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`.

The articles [5], [7], [2], [3], [8], [1], [6], [11], [9], [10], and [4] provide the terminology and notation for this paper.

1. Preliminaries

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

(Def. 1) For all elements a, b, c of L such that $a+b=a+c$ holds $b=c$.

We say that L is add-right-cancelable if and only if:

(Def. 2) For all elements a, b, c of L such that $b+a=c+a$ holds $b=c$.

We say that L is add-cancelable if and only if:

(Def. 3) 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 check the following observations:

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

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

ISSN 1426–2630

* 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.

One can verify 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 observe that every non empty loop structure which is right zeroed, right complementable, and add-associative is also add-right-cancelable.

Let us observe 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.

We now 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 $0_R \cdot a = 0_R$.

(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 $\mathcal{A} \leqslant i$ holds $\mathcal{P}[i]$

provided the following conditions are satisfied:

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

The scheme *RecDef1* deals with a non empty set $\mathcal{A}$, an element $\mathcal{B}$ of $\mathcal{A}$, and a binary operation $\mathcal{C}$ on $\mathcal{A}$, and states that:

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

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

for all values of the parameters.

The scheme *RecDef2* deals with a non empty set $\mathcal{A}$, an element $\mathcal{B}$ of $\mathcal{A}$, and a binary operation $\mathcal{C}$ on $\mathcal{A}$, and states that:

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

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

for all values of the parameters.

2. On Finite Sequences

One can prove the following 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 $p + q$ yields a finite sequence of elements of the carrier of R and is defined by:

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

The following proposition is true

(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 yielding an element of R is defined as follows:

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

We now state several 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 yielding a function from $[: \mathbb{N}, \text{the carrier of } R :]$ into the carrier of R is defined by:

(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 yields a function from $[: \text{the carrier of } R, \mathbb{N} :]$ into the carrier of R and is defined by:

(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 by:

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

The functor $a \cdot n$ yields an element of R and 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 $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle_i = \binom{n}{m} \cdot a^l \cdot b^m$.

The following four propositions are true:

(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. *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] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[5] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.
[6] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[7] Wojciech Skaba and Michał Muzalewski. From double loops to fields. *Formalized Mathematics*, 2(**1**):185–191, 1991.
[8] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[9] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[10] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[11] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 20, 2000