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

Hilbert Basis Theorem[1]

Jonathan Backer
University of Alberta
Edmonton

Piotr Rudnicki
University of Alberta
Edmonton

Summary. We prove the Hilbert basis theorem following [5], page 145. First we prove the theorem for the univariate case and then for the multivariate case. Our proof for the latter is slightly different than in [5]. As a base case we take the ring of polynomilas with no variables. We also prove that a polynomial ring with infinite number of variables is not Noetherian.

MML Identifier: HILBASIS.

The terminology and notation used in this paper are introduced in the following papers: [18], [19], [31], [13], [7], [4], [28], [12], [8], [9], [27], [1], [25], [2], [21], [3], [26], [22], [24], [16], [20], [23], [6], [32], [33], [29], [14], [30], [11], [15], [17], and [10].

1. Preliminaries

One can prove the following propositions:

(1) Let A, B be finite sequences and f be a function. Suppose $\operatorname{rng} A \cup \operatorname{rng} B \subseteq \operatorname{dom} f$. Then there exist finite sequences f_1, f_2 such that $f_1 = f \cdot A$ and $f_2 = f \cdot B$ and $f \cdot (A \frown B) = f_1 \frown f_2$.

(2) For every bag b of 0 holds $\operatorname{decomp} b = \langle\langle \emptyset, \emptyset \rangle\rangle$.

(3) For all natural numbers i, j and for every bag b of j such that $i \leqslant j$ holds $b \restriction i$ is an element of $\operatorname{Bags} i$.

(4) Let i, j be sets, b_1, b_2 be bags of j, and b_1', b_2' be bags of i. If $b_1' = b_1 \restriction i$ and $b_2' = b_2 \restriction i$ and b_1 divides b_2, then b_1' divides b_2'.

[1] This work has been partially supported by NSERC grant OGP9207.

ISSN 1426–2630

(5) Let i, j be sets, b_1, b_2 be bags of j, and b'_1, b'_2 be bags of i. If $b'_1 = b_1 \restriction i$ and $b'_2 = b_2 \restriction i$, then $(b_1 -' b_2) \restriction i = b'_1 -' b'_2$ and $(b_1 + b_2) \restriction i = b'_1 + b'_2$.

Let n, k be natural numbers and let b be a bag of n. The functor b extended by k yields an element of $\operatorname{Bags} n + 1$ and is defined as follows:

(Def. 1) (b extended by k)$\restriction n = b$ and (b extended by k)$(n) = k$.

We now state two propositions:

(6) For every natural number n holds $\operatorname{EmptyBag} n + 1 = \operatorname{EmptyBag} n$ extended by 0.

(7) For every ordinal number n and for all bags b, b_1 of n holds $b_1 \in \operatorname{rng} \operatorname{divisors} b$ iff b_1 divides b.

Let X be a set and let x be an element of X. The functor $\operatorname{UnitBag} x$ yields an element of $\operatorname{Bags} X$ and is defined as follows:

(Def. 2) $\operatorname{UnitBag} x = \operatorname{EmptyBag} X +\cdot (x, 1)$.

Next we state four propositions:

(8) For every non empty set X and for every element x of X holds $\operatorname{support} \operatorname{UnitBag} x = \{x\}$.

(9) Let X be a non empty set and x be an element of X. Then $(\operatorname{UnitBag} x)(x) = 1$ and for every element y of X such that $x \neq y$ holds $(\operatorname{UnitBag} x)(y) = 0$.

(10) For every non empty set X and for all elements x_1, x_2 of X such that $\operatorname{UnitBag} x_1 = \operatorname{UnitBag} x_2$ holds $x_1 = x_2$.

(11) Let X be a non empty ordinal number, x be an element of X, L be a unital non trivial non empty double loop structure, and e be a function from X into L. Then $\operatorname{eval}(\operatorname{UnitBag} x, e) = e(x)$.

Let X be a set, let x be an element of X, and let L be a unital non empty multiplicative loop with zero structure. The functor $1\_1(x, L)$ yielding a Series of X, L is defined by:

(Def. 3) $1\_1(x, L) = 0\_(X, L) +\cdot (\operatorname{UnitBag} x, 1_L)$.

One can prove the following propositions:

(12) Let X be a set, L be a unital non trivial non empty double loop structure, and x be an element of X. Then $(1\_1(x, L))(\operatorname{UnitBag} x) = 1_L$ and for every bag b of X such that $b \neq \operatorname{UnitBag} x$ holds $(1\_1(x, L))(b) = 0_L$.

(13) Let X be a set, x be an element of X, and L be an add-associative right zeroed right complementable unital right distributive non trivial non empty double loop structure. Then $\operatorname{Support} 1\_1(x, L) = \{\operatorname{UnitBag} x\}$.

Let X be an ordinal number, let x be an element of X, and let L be an add-associative right zeroed right complementable unital right distributive non trivial non empty double loop structure. Observe that $1\_1(x, L)$ is finite-Support.

One can prove the following three propositions:

(14) Let L be an add-associative right zeroed right complementable unital right distributive non trivial non empty double loop structure, X be a non empty set, and x_1, x_2 be elements of X. If $1\_1(x_1, L) = 1\_1(x_2, L)$, then $x_1 = x_2$.

(15) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure, x be an element of the carrier of Polynom-Ring L, and p be a sequence of L. If $x = p$, then $-x = -p$.

(16) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure, x, y be elements of the carrier of Polynom-Ring L, and p, q be sequences of L. If $x = p$ and $y = q$, then $x - y = p - q$.

Let L be a right zeroed add-associative right complementable unital distributive non empty double loop structure and let I be a non empty subset of the carrier of Polynom-Ring L. The functor minlen I yields a non empty subset of I and is defined by:

(Def. 4) $\operatorname{minlen} I = \{x; x \text{ ranges over elements of } I\colon \bigwedge_{x',y'\colon \text{Polynomial of } L} (x' = x \wedge y' \in I \Rightarrow \operatorname{len} x' \leqslant \operatorname{len} y')\}$.

We now state the proposition

(17) Let L be a right zeroed add-associative right complementable unital distributive non empty double loop structure, I be a non empty subset of the carrier of Polynom-Ring L, and i_1, i_2 be Polynomials of L. If $i_1 \in \operatorname{minlen} I$ and $i_2 \in I$, then $i_1 \in I$ and $\operatorname{len} i_1 \leqslant \operatorname{len} i_2$.

Let L be a right zeroed add-associative right complementable unital distributive non empty double loop structure, let n be a natural number, and let a be an element of the carrier of L. The functor monomial(a, n) yields a Polynomial of L and is defined as follows:

(Def. 5) For every natural number x holds if $x = n$, then $(\text{monomial}(a, n))(x) = a$ and if $x \neq n$, then $(\text{monomial}(a, n))(x) = 0_L$.

The following four propositions are true:

(18) Let L be a right zeroed add-associative right complementable unital distributive non empty double loop structure, n be a natural number, and a be an element of the carrier of L. Then if $a \neq 0_L$, then $\operatorname{len} \text{monomial}(a, n) = n + 1$ and if $a = 0_L$, then $\operatorname{len} \text{monomial}(a, n) = 0$ and $\operatorname{len} \text{monomial}(a, n) \leqslant n + 1$.

(19) Let L be a right zeroed add-associative right complementable unital distributive non empty double loop structure, n, x be natural numbers, a be an element of the carrier of L, and p be a Polynomial of L. Then $(\text{monomial}(a, n) * p)(x + n) = a \cdot p(x)$.

(20) Let L be a right zeroed add-associative right complementable unital distributive non empty double loop structure, n, x be natural numbers,

a be an element of the carrier of L, and p be a Polynomial of L. Then $(p * \mathrm{monomial}(a, n))(x + n) = p(x) \cdot a$.

(21) Let L be a right zeroed add-associative right complementable unital distributive non empty double loop structure and p, q be Polynomials of L. Then $\mathrm{len}(p * q) \leqslant (\mathrm{len}\, p + \mathrm{len}\, q) -' 1$.

2. On Ring Isomorphism

The following propositions are true:

(22) Let R, S be non empty double loop structures, I be an ideal of R, and P be a map from R into S. If P is a ring isomorphism, then $P^{\circ}I$ is an ideal of S.

(23) Let R, S be add-associative right zeroed right complementable non empty double loop structures and f be a map from R into S. If f is a ring homomorphism, then $f(0_R) = 0_S$.

(24) Let R, S be add-associative right zeroed right complementable non empty double loop structures, F be a non empty subset of the carrier of R, G be a non empty subset of the carrier of S, P be a map from R into S, l_1 be a linear combination of F, L_1 be a linear combination of G, and E be a finite sequence of elements of $[:$the carrier of R, the carrier of R, the carrier of $R:]$. Suppose that

(i) P is a ring homomorphism,

(ii) $\mathrm{len}\, l_1 = \mathrm{len}\, L_1$,

(iii) E represents l_1, and

(iv) for every set i such that $i \in \mathrm{dom}\, L_1$ holds $L_1(i) = P((E_i)_{\mathbf{1}}) \cdot P((E_i)_{\mathbf{2}}) \cdot P((E_i)_{\mathbf{3}})$.

Then $P(\sum l_1) = \sum L_1$.

(25) Let R, S be non empty double loop structures and P be a map from R into S. Suppose P is a ring isomorphism. Then there exists a map P_1 from S into R such that P_1 is a ring isomorphism and $P_1 = P^{-1}$.

(26) Let R, S be Abelian add-associative right zeroed right complementable associative distributive well unital non empty double loop structures, F be a non empty subset of the carrier of R, and P be a map from R into S. If P is a ring isomorphism, then $P^{\circ}F$–ideal $= (P^{\circ}F)$–ideal.

(27) Let R, S be Abelian add-associative right zeroed right complementable associative distributive well unital non empty double loop structures and P be a map from R into S. If P is a ring isomorphism and R is Noetherian, then S is Noetherian.

(28) Let R be an add-associative right zeroed right complementable associative distributive well unital non trivial non empty double loop structure. Then there exists a map from R into Polynom-Ring$(0, R)$ which is a ring isomorphism.

(29) Let R be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, n be a natural number, b be a bag of n, p_1 be a Polynomial of n, R, and F be a finite sequence of elements of the carrier of Polynom-Ring(n, R). Suppose $p_1 = \sum F$. Then there exists a function g from the carrier of Polynom-Ring(n, R) into the carrier of R such that for every Polynomial p of n, R holds $g(p) = p(b)$ and $p_1(b) = \sum(g \cdot F)$.

Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure and let n be a natural number. The functor upm(n, R) yielding a map from Polynom-Ring Polynom-Ring(n, R) into Polynom-Ring$(n+1, R)$ is defined by the condition (Def. 6).

(Def. 6) Let p_1 be a Polynomial of Polynom-Ring(n, R), p_2 be a Polynomial of n, R, p_3 be a Polynomial of $n + 1$, R, and b be a bag of $n + 1$. If $p_3 = (\mathrm{upm}(n, R))(p_1)$ and $p_2 = p_1(b(n))$, then $p_3(b) = p_2(b\restriction n)$.

Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure and let n be a natural number. One can verify the following observations:

* upm(n, R) is additive,
* upm(n, R) is multiplicative,
* upm(n, R) is unity-preserving, and
* upm(n, R) is one-to-one.

Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure and let n be a natural number. The functor mpu(n, R) yields a map from Polynom-Ring$(n + 1, R)$ into Polynom-Ring Polynom-Ring(n, R) and is defined by the condition (Def. 7).

(Def. 7) Let p_1 be a Polynomial of $n + 1$, R, p_2 be a Polynomial of n, R, p_3 be a Polynomial of Polynom-Ring(n, R), i be a natural number, and b be a bag of n. If $p_3 = (\mathrm{mpu}(n, R))(p_1)$ and $p_2 = p_3(i)$, then $p_2(b) = p_1(b$ extended by $i)$.

Next we state two propositions:

(30) Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure, n be a natural number, and p be an element of the

carrier of Polynom-Ring$(n+1, R)$. Then $(\mathrm{upm}(n, R))((\mathrm{mpu}(n, R))(p)) = p$.

(31) Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure and n be a natural number. Then there exists a map from Polynom-Ring Polynom-Ring(n, R) into Polynom-Ring$(n+1, R)$ which is a ring isomorphism.

3. Hilbert Basis Theorem

Let R be a Noetherian Abelian add-associative right zeroed right complementable associative distributive well unital commutative non empty double loop structure. Observe that Polynom-Ring R is Noetherian.

One can prove the following propositions:

(32) Let R be a Noetherian Abelian add-associative right zeroed right complementable associative distributive well unital commutative non empty double loop structure. Then Polynom-Ring R is Noetherian.

(33) Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital non trivial commutative non empty double loop structure. Suppose R is Noetherian. Let n be a natural number. Then Polynom-Ring(n, R) is Noetherian.

(34) Every field is Noetherian.

(35) For every field F and for every natural number n holds Polynom-Ring(n, F) is Noetherian.

(36) Let R be an Abelian right zeroed add-associative right complementable well unital distributive associative commutative non trivial non empty double loop structure and X be an infinite ordinal number. Then Polynom-Ring(X, R) is non Noetherian.

References

[1] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[5] Thomas Becker and Volker Weispfenning. *Gröbner bases: A Computational Approach to Commutative Algebra*. Springer-Verlag, New York, Berlin, 1993.
[6] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[7] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.
[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[11] Agata Darmochwał. Families of subsets, subspaces and mappings in topological spaces. *Formalized Mathematics*, 1(**2**):257–261, 1990.
[12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[13] Agata Darmochwał and Andrzej Trybulec. Similarity of formulae. *Formalized Mathematics*, 2(**5**):635–642, 1991.
[14] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.
[15] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[16] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.
[17] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[18] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.
[19] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[20] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[21] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[22] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[23] Christoph Schwarzweller. The field of quotients over an integral domain. *Formalized Mathematics*, 7(**1**):69–79, 1998.
[24] Christoph Schwarzweller and Andrzej Trybulec. The evaluation of multivariate polynomials. *Formalized Mathematics*, 9(**2**):331–338, 2001.
[25] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[26] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[27] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 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] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[33] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 27, 2000