JOURNAL OF FORMALIZED MATHEMATICS
Volume 12, Released 2000, Published 2003
Inst. of Computer Science, Univ. 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 [7], 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 [7]. 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`.

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

The articles [31], [11], [38], [18], [19], [33], [13], [39], [17], [9], [5], [20], [6], [27], [34], [3], [40], [35], [10], [15], [32], [12], [14], [37], [2], [28], [30], [22], [26], [36], [24], [25], [23], [1], [16], [8], [4], [21], and [29] provide the notation and terminology for this paper.

1. PRELIMINARIES

The following propositions are true:

(1) Let A, B be finite sequences and f be a function. Suppose $\mathrm{rng}\,A \cup \mathrm{rng}\,B \subseteq \mathrm{dom}\,f$. 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 $\mathrm{decomp}\,b = \langle \langle \emptyset, \emptyset \rangle \rangle$.

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

(4) For all sets i, j and for all bags b_1, b_2 of j and for all bags b'_1, b'_2 of i such that $b'_1 = b_1 \restriction i$ and $b'_2 = b_2 \restriction i$ and $b_1 \mid b_2$ holds $b'_1 \mid b'_2$.

(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 $b\,\mathrm{extended\,by}\,k$ yields an element of $\mathrm{Bags}(n+1)$ and is defined as follows:

(Def. 1) $(b\,\mathrm{extended\,by}\,k) \restriction n = b$ and $(b\,\mathrm{extended\,by}\,k)(n) = k$.

The following two propositions are true:

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

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

---

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

Let X be a set and let x be an element of X. The functor $\mathrm{UnitBag}\,x$ yielding an element of $\mathrm{Bags}\,X$ is defined by:

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

We now state four propositions:

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

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

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

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 as follows:

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

We now state two 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 $(1\_1(x,L))(\mathrm{UnitBag}\,x) = 1_L$ and for every bag b of X such that $b \neq \mathrm{UnitBag}\,x$ 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 $\mathrm{Support}\,1\_1(x,L) = \{\mathrm{UnitBag}\,x\}$.

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. One can verify 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 $\mathrm{Polynom\text{-}Ring}\,L$, 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 $\mathrm{Polynom\text{-}Ring}\,L$, 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 $\mathrm{Polynom\text{-}Ring}\,L$. The functor $\mathrm{minlen}\,I$ yielding a non empty subset of I is defined by:

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

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 $\mathrm{Polynom\text{-}Ring}\,L$, and i_1, i_2 be polynomials of L. If $i_1 \in \mathrm{minlen}\,I$ and $i_2 \in I$, then $i_1 \in I$ and $\mathrm{len}\,i_1 \leq \mathrm{len}\,i_2$.

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 L. The functor $\mathrm{monomial}(a,n)$ yielding a polynomial of L is defined by:

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

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 L. Then if $a \neq 0_L$, then $\mathrm{len}\,\mathrm{monomial}(a,n) = n+1$ and if $a = 0_L$, then $\mathrm{len}\,\mathrm{monomial}(a,n) = 0$ and $\mathrm{len}\,\mathrm{monomial}(a,n) \leq n+1$.

(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 L, and p be a polynomial of L. Then $(\mathrm{monomial}(a,n) * p)(x+n) = a \cdot p(x)$.

(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 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 $\mathrm{len}(p*q) \leq (\mathrm{len}\,p + \mathrm{len}\,q) -' 1$.

2. ON RING ISOMORPHISM

One can prove the following propositions:

(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 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 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 R, G be a non empty subset 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 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 ring isomorphism. Then there exists a map P_1 from S into R such that P_1 is 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 R, and P be a map from R into S. If P is 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 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 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 $p_2(b) = p_1(b \text{ extended by } i)$.

The following propositions are true:

(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 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 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. One can verify that Polynom-Ring R is Noetherian.

We now state four propositions:

(33)[1] 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. *Journal of Formalized Mathematics*, 12, 2000. `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`.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. `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 and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finseq_1.html`.

[6] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/dtconstr.html`.

[7] Thomas Becker and Volker Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra*. Springer-Verlag, New York, Berlin, 1993.

[8] Józef Białas. Group and field definitions. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/realset1.html`.

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

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

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

[12] Czesław Byliński. Binary operations applied to finite sequences. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseqop.html`.

[13] Czesław Byliński. A classical first order language. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/cqc_lang.html`.

[14] 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`.

[15] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/funct_4.html`.

[16] Agata Darmochwał. Families of subsets, subspaces and mappings in topological spaces. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/tops_2.html`.

[17] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finset_1.html`.

[18] Agata Darmochwał and Andrzej Trybulec. Similarity of formulae. *Journal of Formalized Mathematics*, 3, 1991. `http://mizar.org/JFM/Vol3/cqc_sim1.html`.

[19] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/seqm_3.html`.

[20] 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`.

[21] Robert Milewski. Associated matrix of linear map. *Journal of Formalized Mathematics*, 7, 1995. `http://mizar.org/JFM/Vol7/matrlin.html`.

---

[1] The proposition (32) has been removed.

[22] Robert Milewski. The ring of polynomials. *Journal of Formalized Mathematics*, 12, 2000. `http://mizar.org/JFM/Vol12/polynom3.html`.

[23] 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`.

[24] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequence over ring and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/algseq_1.html`.

[25] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/binarith.html`.

[26] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/pre_topc.html`.

[27] Jan Popiołek. Real normed space. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/normsp_1.html`.

[28] 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`.

[29] Christoph Schwarzweller. The field of quotients over an integral domain. *Journal of Formalized Mathematics*, 10, 1998. `http://mizar.org/JFM/Vol10/quofield.html`.

[30] Christoph Schwarzweller and Andrzej Trybulec. The evaluation of multivariate polynomials. *Journal of Formalized Mathematics*, 12, 2000. `http://mizar.org/JFM/Vol12/polynom2.html`.

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

[32] Andrzej Trybulec. Tuples, projections and Cartesian products. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/mcart_1.html`.

[33] Andrzej Trybulec. Many-sorted sets. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/pboole.html`.

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

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

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

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

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

[39] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relat_1.html`.

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

Received November 27, 2000

Published January 2, 2004