

Hilbert Basis Theorems*

Benjamin Puyobro

Benoît Ballenghien

Burkhart Wolff

Université Paris Saclay, IRT SystemX, LMF, CNRS

March 17, 2025

Contents

1	A Proof of Hilbert Basis Theorems and an Extension to Formal Power Series	2
2	Ring Miscellaneous	3
3	Polynomials Ring Miscellaneous	4
4	The weak Hilbert Basis theorem	5
4.1	Weak Hilbert Basis	6
4.2	Some properties of noetherian rings	6
4.3	Some properties of the polynomial rings regarding ideals and quotients	6
4.4	The isomorphisms between the different models of polynomials	10
5	The Hilbert Basis theorem for Indexed Polynomials Rings	12
5.1	The isomorphism between $A[X_0..X_n]$ and $A[X_0..X_{n-1}][X_n]$.	12
5.2	Preliminaries lemmas	13
5.3	Hilbert Basis theorem	13
6	The Hilbert Basis theorem for Formal Power Series	13
6.1	Preliminaries definition and lemmas	14
6.2	Premises for noetherian ring proof	15
6.3	The Hilbert Basis theorem	19

*This work has been supported by the French government under the "France 2030" program, as part of the SystemX Technological Research Institute within the CVH project.

7	The Real Ring definition	19
8	Examples	20
8.1	Examples of noetherian rings with $\mathbb{Z}$ and $\mathbb{Z}[X]$	20
8.2	Another example with $\mathbb{R}$ and $\mathbb{R}[X]$	21

1 A Proof of Hilbert Basis Theorems and an Extension to Formal Power Series

The Hilbert Basis Theorem is enlisted in the extension of Wiedijk's catalogue "Formalizing 100 Theorems" [4], a well-known collection of challenge problems for the formalisation of mathematics.

In this paper, we present a formal proof of several versions of this theorem in Isabelle/HOL. Hilbert's basis theorem asserts that every ideal of a polynomial ring over a commutative ring has a finite generating family (a finite basis in Hilbert's terminology). A prominent alternative formulation is: every polynomial ring over a Noetherian ring is also Noetherian.

In more detail, the statement and our generalization can be presented as follows:

- **Hilbert's Basis Theorem.** Let $\mathfrak{R}[X]$ denote the ring of polynomials in the indeterminate X over the commutative ring $\mathfrak{R}$. Then $\mathfrak{R}[X]$ is Noetherian iff $\mathfrak{R}$ is.
- **Corollary.** $\mathfrak{R}[X_1, \dots, X_n]$ is Noetherian iff $\mathfrak{R}$ is.
- **Extension.** If $\mathfrak{R}$ is a Noetherian ring, then $\mathfrak{R}[[X]]$ is a Noetherian ring, where $\mathfrak{R}[[X]]$ denotes the formal power series over the ring $\mathfrak{R}$.

We also provide isomorphisms between the three types of polynomial rings defined in HOL-Algebra. Together with the fact that the noetherian property is preserved by isomorphism, we get Hilbert's Basis theorem for all three models. We believe that this technique has a wider potential of applications in the AFP library.

2 Ring Miscellaneous

theory *Ring-Misc*

imports

HOL-Algebra.RingHom

HOL-Algebra.QuotRing

HOL-Algebra.Embedded-Algebras

begin

Some lemmas that may be considered as useful, and that helps for the Hilbert's basis proof

lemma (in *ring*) *carrier-quot*: $\langle \text{ideal } I \ R \implies \text{carrier } (R \ \text{Quot } I) = \{\{y \oplus x \mid y. y \in I\} \mid x. x \in \text{carrier } R\} \rangle$
 $\langle \text{proof} \rangle$

context

fixes *A B h*

assumes *ring-A*: $\langle \text{ring } A \rangle$

assumes *ring-B*: $\langle \text{ring } B \rangle$

assumes *h1*: $\langle h \in \text{ring-iso } A \ B \rangle$

begin

interpretation *ringA*: *ring A*

$\langle \text{proof} \rangle$

interpretation *ringB*: *ring B*

$\langle \text{proof} \rangle$

interpretation *hrh*: *ring-hom-ring A B h*

$\langle \text{proof} \rangle$

lemma *inv-img-exist*: $\langle \forall xa \in \text{carrier } B. \exists y. y \in \text{carrier } A \wedge h \ y = xa \rangle$

$\langle \text{proof} \rangle$

lemma *img-ideal-is-ideal*: **assumes** *j1*: $\langle \text{ideal } I \ A \rangle$

shows $\langle \text{ideal } (h \ ` \ I) \ B \rangle$

$\langle \text{proof} \rangle$

lemma *img-in-carrier-quot*: $\langle \forall x \in \text{carrier } (A \ \text{Quot } I). h \ ` \ x \in \text{carrier } (B \ \text{Quot } (h \ ` \ I)) \rangle$ **if** *j*: $\langle \text{ideal } I \ A \rangle$ **for** *I*

$\langle \text{proof} \rangle$

lemma *f8*: $\langle xa \in \text{carrier } B \wedge xb \in I \implies h(xb \oplus_A \text{inv-into } (\text{carrier } A) \ h \ xa) = h \ xb \oplus_B xa \rangle$ **if** *j*: $\langle \text{ideal } I \ A \rangle$ **for** *I* *xb xa*

$\langle \text{proof} \rangle$

lemma *f9*: $\langle \forall xa \in \text{carrier } B. \forall xb \in \text{carrier } A. \exists y. h \ y = h \ xb \oplus_B xa \rangle$

$\langle \text{proof} \rangle$

lemma *img-over-set-is-iso*: $\langle \text{ideal } I \ A \implies ((\cdot) \ h) \in \text{ring-iso } (A \ \text{Quot } I) \ (B \ \text{Quot } (h'I)) \rangle$ **for** I
 $\langle \text{proof} \rangle$
end

lemma *Quot-iso-cgen*: $\langle a \in \text{carrier } A \wedge b \in \text{carrier } B \wedge \text{cring } A \wedge \text{cring } B \wedge h \in \text{ring-iso } A \ B \wedge h(a) = b \implies A \ \text{Quot } (\text{cgenideal } A \ a) \simeq B \ \text{Quot } (\text{cgenideal } B \ b) \rangle$
 $\langle \text{proof} \rangle$

end

3 Polynomials Ring Miscellaneous

theory *Polynomials-Ring-Misc*

imports *HOL-Algebra.Polynomials*

begin

Some lemmas that may be considered as useful, and that helps for the Hilbert's basis proof

definition(**in** *ring*) *deg-poly-set*: $\langle \text{deg-poly-set } S \ k = \{a. a \in S \wedge \text{degree } a = k\} \cup \{\emptyset\} \rangle$

definition (**in** *ring*) *lead-coeff-set*: $\langle 'a \text{ list set} \Rightarrow \text{nat} \Rightarrow 'a \text{ set} \rangle$
where $\langle \text{lead-coeff-set } S \ k \equiv \{\text{coeff } a \ (\text{degree } a) \mid a. a \in \text{deg-poly-set } S \ k\} \rangle$

lemma *rule-union*: $\langle x \in (\bigcup_{n \leq k}. A \ l \ n) \longleftrightarrow (\exists n \leq k. x \in A \ l \ n) \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *ring*) *add-0-eq-0-is-0*: $\langle a \in \text{carrier } ((\text{carrier } R)[X]) \implies \emptyset \oplus_{(\text{carrier } R)} [X] \ a = \emptyset \implies a = \emptyset \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *domain*) *inv-coeff-sum*: $\langle a \in \text{carrier } ((\text{carrier } R)[X]) \implies aa \in \text{carrier } ((\text{carrier } R)[X]) \implies a \oplus_{(\text{carrier } R)[X]} aa = \emptyset \longleftrightarrow (\forall n. \text{coeff } a \ n = \text{inv}_{\text{add-monoid } R} (\text{coeff } aa \ n)) \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *ring*) *coeffs-of-add-poly*: $\langle a \in \text{carrier } ((\text{carrier } R)[X]) \implies aa \in \text{carrier } ((\text{carrier } R)[X]) \implies \text{coeff } (a \oplus_{(\text{carrier } R)[X]} aa) \ n = \text{coeff } a \ n \oplus \text{coeff } aa \ n \rangle$

⟨proof⟩

lemma (in ring) length-add:⟨ $a \in \text{carrier}((\text{carrier } R)[X]) \implies aa \in \text{carrier}((\text{carrier } R)[X])$
 $\implies \text{coeff } a (\text{degree } a) \neq \text{inv_add-monoid } R \text{ coeff } aa (\text{degree } aa)$
 $\implies \text{degree } (a \oplus_{(\text{carrier } R)[X]} aa) = \max (\text{degree } a) (\text{degree } aa)$ ⟩
 ⟨proof⟩

lemma (in domain) inv-imp-zero:⟨ $a \in \text{carrier}((\text{carrier } R)[X]) \implies a \oplus_{(\text{carrier } R)[X]} a = []$ ⟩
 ⟨proof⟩

lemma (in domain) R-subdom:⟨subdomain (carrier R) R⟩
 ⟨proof⟩

lemma (in domain) lead-coeff-in-carrier:
 ⟨ideal I ((carrier R)[X]) $\implies a \in I \implies \text{coeff } a (\text{degree } a) \in (\text{carrier } R)$ ⟩ for I a
 ⟨proof⟩

lemma (in domain) degree-of-inv:⟨ $p \in \text{carrier}((\text{carrier } R)[X]) \implies \text{degree } (\text{inv_add-monoid } ((\text{carrier } R)[X]) p) = \text{degree } p$ ⟩ for p
 ⟨proof⟩

lemma (in domain) inv-in-deg-poly-set:⟨ideal I ((carrier R)[X]) $\implies a \in \text{deg-poly-set } I k$
 $\implies \text{inv_add-monoid } ((\text{carrier } R)[X]) a \in \text{deg-poly-set } I k$ ⟩ for I k a
 ⟨proof⟩

lemma (in domain) ideal-lead-coeff-set:⟨ideal (lead-coeff-set I k) R⟩
 if h':⟨ideal I ((carrier R)[X])⟩ for I k
 ⟨proof⟩

lemma (in ring) deg-poly-set-0:⟨deg-poly-set x' 0 = {[a] | a. [a] ∈ x'} ∪ {[]}⟩ for x':⟨'c list set⟩
 ⟨proof⟩

lemma (in ring) lead-coeff-set-0:⟨lead-coeff-set x' 0 = {a. [a] ∈ x'} ∪ {0}⟩ for x'
 ⟨proof⟩

end

4 The weak Hilbert Basis theorem

theory Weak-Hilbert-Basis

imports

HOL-Algebra.Polynomials

HOL-Algebra.Indexed-Polynomials
Polynomials-Ring-Misc
Padic-Field.Cring-Multivariable-Poly
HOL-Algebra.Module
Ring-Misc
begin

In this section, we show what we called "weak" Hilbert basis theorem, meaning Hilbert basis theorem for univariate polynomials. The theorem is done for all three (Polynomials, UP, IP with $\text{card} = 1$) models of polynomials that exists in HOL-Algebra

4.1 Weak Hilbert Basis

lemma (in *noetherian-domain*) *weak-Hilbert-basis*: $\langle \text{noetherian-ring } ((\text{carrier } R)[X]) \rangle$
 $\langle \text{proof} \rangle$

4.2 Some properties of noetherian rings

Assuming I is an ideal of A and A is noetherian, then A/I is noetherian.

lemma *noetherian-ring-imp-quot-noetherian-ring*:
assumes $h1: \langle \text{noetherian-ring } A \rangle$ **and** $h2: \langle \text{ideal } I \ A \rangle$
shows $\langle \text{noetherian-ring } (A \ \text{Quot } I) \rangle$
 $\langle \text{proof} \rangle$

If A is noetherian and $A \simeq B$ then B is noetherian.

lemma *noetherian-isom-imp-noetherian*:
assumes $h1: \langle \text{noetherian-ring } A \wedge \text{ring } B \wedge A \simeq B \rangle$
shows $\langle \text{noetherian-ring } B \rangle$
 $\langle \text{proof} \rangle$

lemma (in *domain*) *subring*: $\langle \text{subring } (\text{carrier } R) \ R \rangle$
 $\langle \text{proof} \rangle$

4.3 Some properties of the polynomial rings regarding ideals and quotients

lemma (in *domain*) *gen-is-cgen*: $\langle (\text{genideal } ((\text{carrier } R)[X]) \ \{X\}) = \text{cgenideal } ((\text{carrier } R)[X]) \ X \rangle$
 $\langle \text{proof} \rangle$

lemma (in *domain*) *principal-X*: $\langle \text{principalideal } (\text{genideal } ((\text{carrier } R)[X]) \ \{X\}) ((\text{carrier } R)[X]) \rangle$
 $\langle \text{proof} \rangle$

named-theorems *poly*

lemma (in *ring*) *PIdl-X[poly]*:

$\langle (cgenideal ((carrier\ R)[X])\ X) = \{a \otimes_{(carrier\ R)\ [X]} X \mid a. a \in carrier((carrier\ R)[X])\} \rangle$
 $\langle proof \rangle$

lemma (in domain) *Idl-X[poly]*:
 $\langle (genideal ((carrier\ R)[X])\ \{X\}) = \{a \otimes_{(carrier\ R)\ [X]} X \mid a. a \in carrier((carrier\ R)[X])\} \rangle$
 $\langle proof \rangle$

lemma (in domain) *Idl-X-is-X[poly]*:
 $\langle p \in (genideal ((carrier\ R)[X])\ \{X\}) \implies \exists a \in carrier((carrier\ R)[X]). p = a \otimes_{(carrier\ R)\ [X]} X \rangle$
 $\langle proof \rangle$

lemma (in ring) *degree-of-nonempty-p[poly]*: $\langle a \in carrier((carrier\ R)[X]) \wedge a \neq [] \implies coeff\ a\ (degree\ a) \neq 0 \rangle$
 $\langle proof \rangle$

lemma (in domain) *coeff-0-of-mult-X[poly]*: $\langle a \in carrier((carrier\ R)[X]) \implies coeff\ (a \otimes_{(carrier\ R)\ [X]} X)\ 0 = 0 \rangle$
 $\langle proof \rangle$

lemma (in domain) *zero-coeff-of-Idl-X[poly]*: $\langle p \in genideal ((carrier\ R)[X])\ \{X\} \implies coeff\ p\ 0 = 0 \rangle$
 $\langle proof \rangle$

lemma (in domain) *mult-X-append-0[poly]*: $\langle p \in carrier((carrier\ R)[X]) \implies p \neq [] \implies poly-mult\ p\ X = p @ [0] \rangle$
 $\langle proof \rangle$

lemma (in ring) *polynomial-incl'*: $\langle p \in carrier((carrier\ R)[X]) \implies set\ p \subseteq (carrier\ R) \rangle$ for p
 $\langle proof \rangle$

lemma (in ring) *hd-in-carrier*: $\langle p \neq [] \implies p \in carrier((carrier\ R)[X]) \implies hd\ p \in (carrier\ R) \rangle$ for p
 $\langle proof \rangle$

lemma (in ring) *inv-in-carrier*:
 $\langle p \neq [] \implies p \in carrier((carrier\ R)[X]) \implies (inv_{add-monoid\ R}\ (hd\ p)) \in (carrier\ R) \rangle$
for p
 $\langle proof \rangle$

lemma (in ring) *inv-ld-coeff*:
 $\langle p \neq [] \implies p \in carrier((carrier\ R)[X]) \implies (inv_{add-monoid\ R}\ (hd\ p)) \# replicate\ (degree\ p)\ 0 \in carrier((carrier\ R)[X]) \rangle$
for p
 $\langle proof \rangle$

lemma (in ring) take-in-RX: $\langle p \in \text{carrier}((\text{carrier } R)[X]) \implies n \leq \text{length } p \implies (\text{set } (\text{take } n \ p)) \subseteq (\text{carrier } R) \rangle$ for $p \ n$
 $\langle \text{proof} \rangle$

lemma (in ring) normalize-take-is-poly: $\langle p \in \text{carrier}((\text{carrier } R)[X]) \implies n \leq \text{length } p \implies \text{normalize } (\text{take } n \ p) \in \text{carrier}((\text{carrier } R)[X]) \rangle$ for $n \ p$
 $\langle \text{proof} \rangle$

lemma (in ring) normalize-take-is-take: $\langle p \in \text{carrier}((\text{carrier } R)[X]) \wedge n \leq \text{length } p \implies \text{normalize } (\text{take } n \ p) = \text{take } n \ p \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) take-in-carrier: $\langle p \in \text{carrier}((\text{carrier } R)[X]) \implies n \leq \text{length } p \implies (\text{take } n \ p) \in \text{carrier}((\text{carrier } R)[X]) \rangle$
 $\langle \text{proof} \rangle$

lemma (in domain) take-misc-poly: $\langle p \in \text{carrier}((\text{carrier } R)[X]) \implies p \neq [] \implies \text{coeff } p \ 0 = \mathbf{0} \implies ((\text{take } (\text{degree } p) \ p)) \otimes_{(\text{carrier } R)} [X] X = p \rangle$ for p
 $\langle \text{proof} \rangle$

lemma (in ring) length-geq-2: $\langle \text{normalize } p \neq [] \wedge \neg(\exists a. \text{normalize } p = [a]) \implies \text{length } p \geq 2 \rangle$ for p : $\langle 'a \text{ list} \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) norm-take-not-mt: $\langle \text{length } (\text{normalize } p) \geq 2 \implies \text{normalize } (\text{take } (\text{degree } p) \ p) \neq [] \rangle$ for p : $\langle 'a \text{ list} \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) normalize-take-invariant: $\langle p \in \text{carrier}((\text{carrier } R)[X]) \implies p \neq [] \implies (\text{normalize } (\text{take } (\text{degree } p) \ p)) @ [\text{coeff } p \ 0] = p \rangle$ for p
 $\langle \text{proof} \rangle$

lemma (in domain) lower-coeff-add: $\langle p \neq [] \implies p \in \text{carrier}((\text{carrier } R)[X]) \wedge b \in (\text{carrier } R) \implies \text{coeff } (((\text{normalize } p) @ [\mathbf{0}]) \oplus_{(\text{carrier } R)} [X] [b]) = \text{coeff } ((\text{normalize } p) @ [b]) \rangle$ for $p \ b$
 $\langle \text{proof} \rangle$

lemma (in ring) cons-in-RX: $\langle a @ p \in \text{carrier}((\text{carrier } R)[X]) \implies \text{normalize } p \in \text{carrier}((\text{carrier } R)[X]) \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) p-in-norm: $\langle p \in \text{carrier}((\text{carrier } R)[X]) \implies \text{normalize } p = p \rangle$
 $\langle \text{proof} \rangle$

lemma (in domain) lower-coeff-add': $\langle p \neq [] \implies p \in \text{carrier}((\text{carrier } R)[X]) \wedge b \in$

$(\text{carrier } R) \implies (((\text{normalize } p) @[\mathbf{0}]) \oplus_{(\text{carrier } R) [X]} [b]) = ((\text{normalize } p) @[b])$
for $p \ b$
 $\langle \text{proof} \rangle$

lemma (in domain) *poly-invariant*: $\langle p \in \text{carrier}((\text{carrier } R)[X]) \implies p \neq [] \implies ((\text{normalize } (\text{take } (\text{degree } p) \ p)) \otimes_{(\text{carrier } R) [X]} X) \oplus_{(\text{carrier } R) [X]} [\text{coeff } p \ 0] = p \rangle$
for p
 $\langle \text{proof} \rangle$

lemma (in domain) *gen-ideal-X-iff*: $\langle p \in (\text{genideal } ((\text{carrier } R)[X]) \ \{X\}) \longleftrightarrow (p \in \text{carrier } ((\text{carrier } R)[X]) \wedge \text{coeff } p \ 0 = \mathbf{0}) \rangle$ **for** $p::\langle 'a \text{ list} \rangle$
 $\langle \text{proof} \rangle$

lemma (in domain) *gen-ideal-X-iff'*: $\langle (\text{genideal } ((\text{carrier } R)[X]) \ \{X\}) = \{p \in \text{carrier } ((\text{carrier } R)[X]). \text{coeff } p \ 0 = \mathbf{0}\} \rangle$ **for** $p::\langle 'a \text{ list} \rangle$
 $\langle \text{proof} \rangle$

lemma (in domain) *quot-X-is-R*: $\langle \text{carrier } (((\text{carrier } R)[X]) \ \text{Quot } (\text{genideal } ((\text{carrier } R)[X]) \ \{X\})) = \{ \{x \in \text{carrier } ((\text{carrier } R)[X]). \text{coeff } x \ 0 = a\} \mid a. a \in (\text{carrier } R) \} \rangle$
 $\langle \text{proof} \rangle$

lemma (in domain) *uniq-a-quot*:
 $\langle c \in \text{carrier } (((\text{carrier } R)[X]) \ \text{Quot } (\text{genideal } ((\text{carrier } R)[X]) \ \{X\})) \implies \exists ! a \in (\text{carrier } R). \forall y \in c. \text{coeff } y \ 0 = a \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) *append-in-carrier*: $\langle a \in \text{carrier}((\text{carrier } R)[X]) \wedge b \in \text{carrier}((\text{carrier } R)[X]) \implies a @ b \in \text{carrier}((\text{carrier } R)[X]) \rangle$
 $\langle \text{proof} \rangle$

lemma (in domain) *The-a-is-a*: $\langle a \in (\text{carrier } R) \implies (\text{THE } aa. \forall y \in \{x \mid x. x \in \text{carrier } ((\text{carrier } R) [X]) \wedge \text{local.coeff } x \ 0 = a\}. \text{local.coeff } y \ 0 = aa) = a \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) *poly-mult-in-carrier2*:
 $\llbracket \text{set } p1 \subseteq \text{carrier } R; \text{set } p2 \subseteq \text{carrier } R \rrbracket \implies \text{poly-mult } p1 \ p2 \in \text{carrier } ((\text{carrier } R)[X])$
 $\langle \text{proof} \rangle$

lemma (in ring) *normalize-equiv*: $\langle \text{polynomial } (\text{carrier } R) (\text{normalize } p) \longleftrightarrow (\text{coeff } (\text{normalize } p)) \in \text{carrier } (UP \ R) \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) *p-in-RX-imp-in-P*: $\langle p \in \text{carrier } ((\text{carrier } R)[X]) \implies \text{coeff } p \in up \ R \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) *X-has-correp*: $\langle \text{coeff } X = (\lambda i. \text{ if } i = 1 \text{ then } \mathbf{1} \text{ else } \mathbf{0}) \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) *mult-is-mult*:
 $\langle \{x, y\} \subseteq \text{carrier } ((\text{carrier } R)[X]) \implies \text{coeff } (x \otimes_{(\text{carrier } R)[X]} y) = \text{coeff } x \otimes_{UP R} \text{coeff } y \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) *add-is-add*: $\langle x \in \text{carrier } (\text{poly-ring } R) \implies$
 $y \in \text{carrier } (\text{poly-ring } R)$
 $\implies \text{coeff } (x \oplus_{\text{poly-ring } R} y) = \text{coeff } x \oplus_{UP R} \text{coeff } y \rangle$
 $\langle \text{proof} \rangle$

4.4 The isomorphisms between the different models of polynomials

lemma (in ring) *coeff-iso-RX-P*: $\langle \text{coeff} \in \text{ring-iso } (\text{poly-ring } R) (UP R) \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) *RX-iso-P*: $\langle (\text{carrier } R)[X] \simeq (UP R) \rangle$
 $\langle \text{proof} \rangle$

lemma (in domain) *R-isom-RX-X*: $\langle R \simeq (((\text{carrier } R)[X]) \text{ Quot } (\text{genideal } ((\text{carrier } R)[X]) \{X\}))) \rangle$
 $\langle \text{proof} \rangle$

lemma (in domain) *RX-imp-RX-over-X*:
 $\langle \text{noetherian-ring } (\text{carrier } R[X]) \implies \text{noetherian-ring } (\text{carrier } R[X] \text{ Quot } \text{genideal } (\text{carrier } R[X]) \{X\}) \rangle$
 $\langle \text{proof} \rangle$

lemma (in domain) *noetherian-RX-imp-noetherian-R*:
 $\langle \text{noetherian-ring } ((\text{carrier } R)[X]) \implies \text{noetherian-ring } R \rangle$
 $\langle \text{proof} \rangle$

lemma *principal-imp-noetherian*: $\langle \text{principal-domain } R \implies \text{noetherian-ring } R \rangle$
 $\langle \text{proof} \rangle$

lemma (in ring) *coeff-iff-poly-carrier*: $\langle x \in \text{carrier } (\text{poly-ring } R) \implies$
 $y \in \text{carrier } (\text{poly-ring } R) \implies (x=y) \longleftrightarrow \text{coeff } x = \text{coeff } y \rangle$
 $\langle \text{proof} \rangle$

lemma *zero-is-zero*: $\langle B = B(\text{zero} := \mathbf{0}_B) \rangle$
 $\langle \text{proof} \rangle$

lemma *ring-iso-imp-iso*: $\langle A \simeq B \implies A \cong B \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *ring*) *iso-imp-exist-0*: $\langle R \simeq B \implies \exists x. \text{ring } (B(\text{zero} := x)) \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *domain*) *noetherian-R-imp-noetherian-UP-R*:
assumes $h1: \langle \text{noetherian-ring } R \rangle$
shows $\langle \text{noetherian-ring } (UP\ R) \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *domain*) *noetheriandom-R-imp-noetheriandom-UP-R*:
assumes $h1: \langle \text{noetherian-domain } R \rangle$
shows $\langle \text{noetherian-domain } (UP\ R) \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *cring*) *Pring-one-index-isom-P*: $\langle (Pring\ R\ \{N\}) \simeq UP\ R \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *cring*) *P-isom-Pring-one-index*: $\langle UP\ R \simeq (Pring\ R\ \{N\}) \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *domain*) *P-iso-RX*: $\langle UP\ R \simeq ((\text{carrier } R)[X]) \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *domain*) *IP-noeth-imp-R-noeth*: $\langle \text{noetherian-ring } (Pring\ R\ \{a\}) \implies \text{noetherian-ring } R \rangle$
 $\langle \text{proof} \rangle$

lemma (**in** *domain*) *R-iso-UPR-quot-X*: $\langle R \simeq (UP\ R)\ \text{Quot } (cgenideal\ (UP\ R))\ (\lambda i. \text{if } i=1 \text{ then } \mathbf{1} \text{ else } \mathbf{0}) \rangle$
 $\langle \text{proof} \rangle$

end

5 The Hilbert Basis theorem for Indexed Polynomials Rings

theory *Hilbert-Basis*

imports *Weak-Hilbert-Basis*

begin

5.1 The isomorphism between $A[X_0..X_n]$ and $A[X_0..X_{n-1}][X_n]$

This part until *var_factor_iso* is due to Aaron Crighton

lemma *ring-iso-memI'*:
assumes $f \in \text{ring-hom } R \ S$
assumes $g \in \text{ring-hom } S \ R$
assumes $\bigwedge x. x \in \text{carrier } R \implies g (f x) = x$
assumes $\bigwedge x. x \in \text{carrier } S \implies f (g x) = x$
shows $f \in \text{ring-iso } R \ S$
 $g \in \text{ring-iso } S \ R$
 $\langle \text{proof} \rangle$

lemma(**in** *cring*) *var-factor-inverse*:
assumes $I = J0 \cup J1$
assumes $J1 \subseteq I$
assumes $J1 \cap J0 = \{\}$
assumes $\psi1 = (\text{var-factor-inv } I \ J0 \ J1)$
assumes $\psi0 = (\text{var-factor } I \ J0 \ J1)$
assumes $P \in \text{carrier } (\text{Pring } (\text{Pring } R \ J0) \ J1)$
shows $\psi0 (\psi1 P) = P$
 $\langle \text{proof} \rangle$

lemma(**in** *cring*) *var-factor-iso*:
assumes $I = J0 \cup J1$
assumes $J1 \subseteq I$
assumes $J1 \cap J0 = \{\}$
assumes $\psi1 = (\text{var-factor-inv } I \ J0 \ J1)$
assumes $\psi0 = (\text{var-factor } I \ J0 \ J1)$
shows $\psi0 \in \text{ring-iso } (\text{Pring } R \ I) (\text{Pring } (\text{Pring } R \ J0) \ J1)$
 $\psi1 \in \text{ring-iso } (\text{Pring } (\text{Pring } R \ J0) \ J1) (\text{Pring } R \ I)$
 $\langle \text{proof} \rangle$

lemma (**in** *cring*) *is-iso-Prings*:
assumes $h1:I = J0 \cup J1$
assumes $h2:J1 \subseteq I$
assumes $h3:J1 \cap J0 = \{\}$

shows $(\text{Pring } (\text{Pring } R \ J0) \ J1) \simeq (\text{Pring } R \ I)$ **and** $(\text{Pring } R \ I) \simeq (\text{Pring } (\text{Pring } R \ J0) \ J1)$
 $\langle \text{proof} \rangle$

5.2 Preliminaries lemmas

lemma (in *cring*) *poly-no-var*:
assumes $\langle x \in ((\text{carrier } R) [\mathcal{X}_{\{\}}]) \wedge xa \neq \{\#\} \rangle$
shows $\langle x \ xa = 0 \rangle$
 $\langle \text{proof} \rangle$

lemma (in *cring*) *R-isom-P-mt*: $\langle R \simeq \text{Pring } R \ \{\} \rangle$
 $\langle \text{proof} \rangle$

5.3 Hilbert Basis theorem

We show after this Hilbert basis theorem, based on Indexed Polynomials in HOL-Algebra and its extension in *PadicFields*

theorem (in *domain*) *Hilbert-basis*:
assumes $h1: \langle \text{noetherian-ring } R \rangle$ **and** $h2: \langle \text{finite } I \rangle$
shows $\langle \text{noetherian-ring } (\text{Pring } R \ I) \rangle$
 $\langle \text{proof} \rangle$

lemma (in *domain*) *R-noetherian-implies-IP-noetherian*:
assumes $h1: \langle \text{noetherian-ring } R \rangle$
shows $\langle \text{noetherian-ring } (\text{Pring } R \ \{0..N::\text{nat}\}) \rangle$
 $\langle \text{proof} \rangle$

lemma (in *domain*) *IP-noetherian-implies-R-noetherian*:
assumes $h1: \langle \text{noetherian-ring } (\text{Pring } R \ I) \rangle$ **and** $h2: \langle \text{finite } I \rangle$
shows $\langle \text{noetherian-ring } R \rangle$
 $\langle \text{proof} \rangle$

end

6 The Hilbert Basis theorem for Formal Power Series

theory *Formal-Power-Series-Ring*

imports
HOL-Library.Extended-Nat
HOL-Computational-Algebra.Formal-Power-Series
HOL-Algebra.Module
HOL-Algebra.Ring-Divisibility

begin

We define the ring of formal power series over a domain (idom) as a record to match HOL-Algebra definitions. We then show that it is a domain for addition and multiplication. This is immediate with the existing theory from HOL-Analysis.

We then proceed to show the theorem similar to Hilbert's basis theorem but for the ring of Formal power series.

6.1 Preliminaries definition and lemmas

context

fixes $R::\langle 'a::\{idom\} \text{ ring} \rangle$ (**structure**)
defines $R::\langle R \equiv \langle \text{carrier} = UNIV, \text{monoid.mult} = (*), \text{one} = 1, \text{zero} = 0, \text{add} = (+) \rangle \rangle$
begin

lemma $\text{ring-}R::\langle \text{ring } R \rangle$
 $\langle \text{proof} \rangle$

lemma $\text{domain-}R::\langle \text{domain } R \rangle$
 $\langle \text{proof} \rangle$

definition

$\text{FPS-ring} :: 'a::\{idom\} \text{ fps ring}$
where $\text{FPS-ring} = \langle \text{carrier} = UNIV, \text{monoid.mult} = (*), \text{one} = 1, \text{zero} = 0, \text{add} = (+) \rangle$

lemma $\text{ring-FPS}::\langle \text{ring FPS-ring} \rangle$
 $\langle \text{proof} \rangle$

lemma $\text{cring-FPS}::\langle \text{cring FPS-ring} \rangle$
 $\langle \text{proof} \rangle$

lemma $\text{domain-FPS}::\langle \text{domain FPS-ring} \rangle$
 $\langle \text{proof} \rangle$

valuation over FPS-ring

definition $v\text{-subdegree} :: ('a::\{idom\}) \text{ fps} \Rightarrow \text{enat}$ **where**
 $v\text{-subdegree } f = (\text{if } f = 0 \text{ then } \infty \text{ else subdegree } f)$

definition $\text{valuation}::\langle 'a::\{idom\} \text{ fps} \Rightarrow \text{enat} \rangle (\nu)$ **where**
 $\nu \ x \equiv \text{Sup } \{ \text{enat } k \mid k. x \in \text{cgenideal FPS-ring } (\text{fps-X}^k) \}$

lemma $\text{fps-X-pow-k-ideal-iff}::\langle \text{cgenideal FPS-ring } (\text{fps-X}^k) = \{x. v\text{-subdegree } x \geq k\} \rangle$
 $\langle \text{proof} \rangle$

lemma *valuation-miscs-1*:**assumes** $h1: \langle f \in \text{carrier FPS-ring} \rangle$
shows $\langle (\text{valuation } f) = (\infty::\text{enat}) \longleftrightarrow f = 0 \rangle$
 $\langle \text{proof} \rangle$

lemma *valuation-miscs-0*:
shows $\langle \text{valuation } f = \text{Inf } \{ \text{enat } n \mid n. \text{fps-nth } f \ n \neq 0 \} \rangle$
 $\langle \text{proof} \rangle$

lemma *valuation-miscs-3*: $\langle \text{valuation } f = v\text{-subdegree } f \rangle$
 $\langle \text{proof} \rangle$

lemma *triangular-ineq-v*: $\langle \text{valuation } (f + g) \geq \min (\text{valuation } f) (\text{valuation } g) \rangle$
 $\langle \text{proof} \rangle$

lemma *triang-eq-v*:**assumes** $h1: \langle \text{valuation } f \neq \text{valuation } g \rangle$
shows $\langle \text{valuation } (f + g) = \min (\text{valuation } f) (\text{valuation } g) \rangle$
 $\langle \text{proof} \rangle$

lemma *prod-triang-v*: $\langle \text{valuation } (f * g) = \text{valuation } f + \text{valuation } g \rangle$
 $\langle \text{proof} \rangle$

6.2 Premisses for noetherian ring proof

definition *subdeg-poly-set*: $\langle \text{subdeg-poly-set } S \ k = \{ a. a \in S \wedge \text{subdegree } a = k \} \cup \{ 0 \} \rangle$

definition *sublead-coeff-set*: $\langle 'b::\{ \text{zero} \} \text{ fps set} \Rightarrow \text{nat} \Rightarrow 'b \text{ set} \rangle$
where $\langle \text{sublead-coeff-set } S \ k \equiv \{ \text{fps-nth } a \ (\text{subdegree } a) \mid a. a \in \text{subdeg-poly-set } S \ k \} \rangle$

lemma *ideal-nonempty*: $\langle \text{ideal } I \text{ FPS-ring} \Rightarrow I \neq \{ \} \rangle$
 $\langle \text{proof} \rangle$

lemma *mult-X-in-ideal*: $\langle \text{ideal } I \text{ FPS-ring} \Rightarrow \forall x \in I. \text{fps-X } * \ x \in I \rangle$
 $\langle \text{proof} \rangle$

lemma *non-empty-sublead*: $\langle \text{ideal } I \text{ FPS-ring} \Rightarrow \text{sublead-coeff-set } I \ k \neq \{ \} \rangle$
 $\langle \text{proof} \rangle$

lemma *inv-unique*: $\langle \forall x \in \text{carrier FPS-ring}. \exists ! y. x + y = 0 \rangle$
 $\langle \text{proof} \rangle$

lemma *inv-same-degree*:**assumes** $h: \langle x \in \text{carrier FPS-ring} \rangle$
shows $\langle \text{subdegree } (\text{inv}_{\text{add-monoid FPS-ring}} x) = \text{subdegree } x \rangle$
 $\langle \text{proof} \rangle$

lemma *inv-subdegree-is-inv*: **assumes** $h: x \in \text{carrier FPS-ring}$
shows $\langle \text{fps-nth } (\text{inv}_{\text{add-monoid FPS-ring}} x) \ (\text{subdegree } x) =$
 $(\text{inv}_{\text{add-monoid } R} (\text{fps-nth } x \ (\text{subdegree } x))) \rangle$

$\langle \text{proof} \rangle$

lemma *subdeg-inv-in-sublead*:

assumes $h1:\langle \text{ideal } I \text{ FPS-ring} \rangle$ **and** $h2:\langle a \in \text{sublead-coeff-set } I \ k \rangle$

shows $\langle \text{inv}_{\text{add-monoid } R} \ a \in \text{sublead-coeff-set } I \ k \rangle$

$\langle \text{proof} \rangle$

lemma *mult-stable-sublead*:

assumes $h1:\langle \text{ideal } I \text{ FPS-ring} \rangle$

and $h2:\langle a \in \text{sublead-coeff-set } I \ k \rangle$

and $h3:\langle b \in \text{sublead-coeff-set } I \ k \rangle$

shows $\langle a \otimes_R b \in \text{sublead-coeff-set } I \ k \rangle$

$\langle \text{proof} \rangle$

lemma *add-stable-sublead*:

assumes $h1:\langle \text{ideal } I \text{ FPS-ring} \rangle$

and $h2:\langle a \in \text{sublead-coeff-set } I \ k \rangle$

and $h3:\langle b \in \text{sublead-coeff-set } I \ k \rangle$

shows $\langle a \otimes_{\text{add-monoid } R} b \in \text{sublead-coeff-set } I \ k \rangle$

$\langle \text{proof} \rangle$

lemma *outer-stable-sublead*:

assumes $h1:\langle \text{ideal } I \text{ FPS-ring} \rangle$ **and** $h2:\langle a \in \text{sublead-coeff-set } I \ k \rangle$ **and** $h3:\langle b \in \text{carrier } R \rangle$

shows $\langle b \otimes a \in \text{sublead-coeff-set } I \ k \rangle$

$\langle \text{proof} \rangle$

lemma *sublead-ideal*: $\langle \text{ideal } I \text{ FPS-ring} \implies \text{ideal } (\text{sublead-coeff-set } I \ k) \ R \rangle$

$\langle \text{proof} \rangle$

lemma *order-sublead*:

assumes $h1:\langle J1 \subseteq J2 \rangle$ **and** $h2:\langle \text{ideal } J1 \text{ FPS-ring} \rangle$ **and** $h3:\langle \text{ideal } J2 \text{ FPS-ring} \rangle$

shows $\langle \text{sublead-coeff-set } J1 \ k \subseteq \text{sublead-coeff-set } J2 \ k \rangle$

$\langle \text{proof} \rangle$

lemma *sup-sublead-stable-add*: $\langle \text{ideal } I \text{ FPS-ring} \implies$

$a \in \bigcup (\text{range } (\text{sublead-coeff-set } I)) \implies$

$b \in \bigcup (\text{range } (\text{sublead-coeff-set } I))$

$\implies a \otimes_{\text{add-monoid } R} b \in \bigcup (\text{range } (\text{sublead-coeff-set } I)) \rangle$

$\langle \text{proof} \rangle$

lemma *sup-sublead-ideal*: $\langle \text{ideal } I \text{ FPS-ring} \implies \text{ideal } (\bigcup k. \text{sublead-coeff-set } I \ k) \ R \rangle$

$\langle \text{proof} \rangle$

lemma *Sub-subdeg-eq-ideal*: $\langle \text{ideal } J \text{ FPS-ring} \implies (\bigcup k. \text{subdeg-poly-set } J \ k) = J \rangle$

$\langle \text{proof} \rangle$

lemma *eq-subdeg*:

assumes $h1: \langle J1 \subseteq J2 \rangle$
and $h3: \langle \text{ideal } J1 \text{ FPS-ring} \rangle$ **and** $h4: \langle \text{ideal } J2 \text{ FPS-ring} \rangle$
shows $\langle J1 = J2 \iff (\forall k. \text{subdeg-poly-set } J1 \ k = \text{subdeg-poly-set } J2 \ k) \rangle$
 $\langle \text{proof} \rangle$

lemma *inculded-sublead*: $\langle \text{ideal } I \text{ FPS-ring} \implies \text{sublead-coeff-set } I \ k \subseteq \text{sublead-coeff-set } I \ (k+1) \rangle$
 $\langle \text{proof} \rangle$

lemma *included-sublead-gen*: **assumes** $\langle \text{ideal } I \text{ FPS-ring} \rangle$ $\langle k \leq k' \rangle$
shows $\langle \text{sublead-coeff-set } I \ k \subseteq \text{sublead-coeff-set } I \ (k') \rangle$
 $\langle \text{proof} \rangle$

lemma *sup-sublead*:
assumes $h1: \langle \text{ideal } I \text{ FPS-ring} \rangle$
and $h2: \langle \text{noetherian-ring } R \rangle$
shows $\langle \bigcup \{ \text{sublead-coeff-set } I \ k \mid k. k \in \text{UNIV} \} \in \{ \text{sublead-coeff-set } I \ k \mid k. k \in \text{UNIV} \} \rangle$
 $\langle \text{proof} \rangle$

lemma *subdeg-inf-imp-s-tendsto-zero*:
fixes $s: \langle \text{nat} \Rightarrow 'a::\{\text{idom}\} \text{fps} \rangle$
assumes $g2: \langle \text{strict-mono } (\lambda n. \text{subdegree } (s \ n)) \rangle$
shows $\langle s \longrightarrow 0 \rangle$
 $\langle \text{proof} \rangle$

lemma *idl-sum*: $\langle \text{finite } A \implies \text{ideal } \{x. \exists s. x = (\sum i \in \{0..<\text{card } A\}. s \ i * \text{from-nat-into } A \ i)\} \ R \rangle$ **for** A
 $\langle \text{proof} \rangle$

lemma *genideal-sum-rep*:
 $\langle \text{finite } A \implies \text{genideal } R \ A = \{x. \exists s. x = (\sum i \in \{0..<\text{card } A\}. s \ i * \text{from-nat-into } A \ i)\} \rangle$ **for** A
 $\langle \text{proof} \rangle$

lemma *fps-sum-rep-nth'*:
 $\text{fps-nth } (\text{sum } (\lambda i. \text{fps-const}(a \ i) * \text{fps-X}^i) \ \{0..m\}) \ n = (\text{if } n \leq m \text{ then } a \ n \text{ else } 0)$
 $\langle \text{proof} \rangle$

lemma *abs-tndsto*: **shows** $\langle (\lambda n. (\sum i \leq n. \text{fps-const } (s \ i) * \text{fps-X}^i)::'a \ \text{fps}) \longrightarrow \text{Abs-fps } s \rangle$
 $\langle \text{is } \langle ?s \longrightarrow ?a \rangle \rangle$
 $\langle \text{proof} \rangle$

lemma *add-stable-FPS-ring*: $\langle \text{ideal } I \text{ FPS-ring} \implies a \in I \implies b \in I \implies a + b \in I \rangle$
 $\langle \text{proof} \rangle$

lemma *abs-tndsto-le*: **shows** $\langle (\lambda n. (\sum i < n. \text{fps-const } (s \ i) * \text{fps-X}^{\wedge} i) :: 'a \ \text{fps})$
 $\longrightarrow \text{Abs-fps } s \rangle$
 $\langle \text{proof} \rangle$

lemma *bij-betw-strict-mono*:
assumes $\langle \text{strict-mono } (f :: \text{nat} \Rightarrow \text{nat}) \rangle$
shows $\langle \text{bij-betw } f \text{ UNIV } (f' \text{ UNIV}) \rangle$
 $\langle \text{proof} \rangle$

lemma *no-i-inf-0*: $\langle \text{strict-mono } (f :: \text{nat} \Rightarrow \text{nat}) \implies i < f \ 0 \implies \neg(\exists j. f \ j = i) \rangle$
 $\langle \text{proof} \rangle$

lemma *inter-mt*: $\langle \text{strict-mono } (f :: \text{nat} \Rightarrow \text{nat}) \implies \{.. < f \ 0\} \cap \text{range } f = \{\} \rangle$
 $\langle \text{proof} \rangle$

lemma *range-inter-f*: $\langle \text{strict-mono } (f :: \text{nat} \Rightarrow \text{nat}) \implies \{.. < f \ n\} \cap \text{range } f = f' \{0.. < n\} \rangle$
 $\langle \text{proof} \rangle$

lemma *simp-rule-sum*: $\langle \text{strict-mono } (f :: \text{nat} \Rightarrow \text{nat}) \implies (\sum i \in \{.. < f \ (\text{Suc } n)\}. (\text{if } i$
 $\in \text{range } f$
 $\text{then } (s \ ((\text{inv-into } \text{UNIV } f) \ i)) * \text{fps-X}^{\wedge} i \text{ else } 0)) = (\sum i \in \{.. < f \ n\}. (\text{if } i \in \text{range}$
 $f \text{ then}$
 $(s \ ((\text{inv-into } \text{UNIV } f) \ i)) * \text{fps-X}^{\wedge} i \text{ else } 0)) + (s \ ((\text{inv-into } \text{UNIV } f) \ (f \ n))) * \text{fps-X}^{\wedge} (f$
 $n)) \rangle$
 $\langle \text{proof} \rangle$

lemma *rewriting-sum*: **assumes** $\langle \text{strict-mono } (f :: \text{nat} \Rightarrow \text{nat}) \rangle$
shows $\langle (\sum i < n. \text{fps-const } (s \ i) * \text{fps-X}^{\wedge} (f \ i))$
 $= (\sum i \in \{.. < f \ n\}. (\text{if } i \in \text{range } f \text{ then } \text{fps-const } (s \ (\text{inv-into } \text{UNIV } f \ i)) * \text{fps-X}^{\wedge} i$
 $\text{else } 0)) \rangle$
 $\langle \text{proof} \rangle$

lemma *exists-seq*: $\langle \text{strict-mono } (f :: \text{nat} \Rightarrow \text{nat}) \implies$
 $\exists s. (\sum i \in \{.. < f \ n\}. (\text{if } i \in \text{range } f \text{ then } \text{fps-const } (s' \ (\text{inv-into } \text{UNIV } f \ i)) * \text{fps-X}^{\wedge} i$
 $\text{else } 0))$
 $= (\sum i \in \{.. < f \ n\}. \text{fps-const } (s \ i) * \text{fps-X}^{\wedge} i) \rangle$
 $\langle \text{proof} \rangle$

lemma *exists-seq'*: $\langle \text{strict-mono } (f :: \text{nat} \Rightarrow \text{nat}) \implies$
 $\exists s. (\sum i < n. \text{fps-const } (s' \ i) * (\text{fps-X} :: 'a \ \text{fps})^{\wedge} (f \ i)) =$
 $(\sum i \in \{.. < f \ n\}. \text{fps-const } (s \ i) * \text{fps-X}^{\wedge} i) \rangle$
 $\langle \text{proof} \rangle$

lemma *exists-seq-all*: $\langle \text{strict-mono } (f::\text{nat} \Rightarrow \text{nat}) \Rightarrow$
 $\exists s. \forall n. (\sum i \in \{..<f\ n\}. (\text{if } i \in \text{range } f \text{ then } \text{fps-const } (s' (\text{inv-into } \text{UNIV } f\ i))$
 $* \text{fps-X}^i \text{ else } 0))$
 $= (\sum i \in \{..<f\ n\}. \text{fps-const } (s\ i) * \text{fps-X}^i)$
 $\rangle$
<proof>

lemma *exists-seq-all'*: $\langle \text{strict-mono } (f::\text{nat} \Rightarrow \text{nat}) \Rightarrow$
 $\exists s. \forall n. (\sum i < n. \text{fps-const } (s' i) * \text{fps-X}^i(f\ i)) =$
 $(\sum i \in \{..<f\ n\}. \text{fps-const } (s\ i) * \text{fps-X}^i)$
 $\rangle$
<proof>

lemma *tendsto-f-seq*:**assumes** $\langle \text{strict-mono } (f::\text{nat} \Rightarrow \text{nat}) \rangle$
shows $\langle (\lambda n. (\sum i \in \{..<f\ n\}. \text{fps-const } (s\ i) * \text{fps-X}^i))::'a\ \text{fps} \rangle \longrightarrow \text{Abs-fps } (\lambda i.$
 $s\ i)$
<proof>

lemma *LIMSEQ-add-fps*:
fixes $x\ y :: 'a::\text{idom}\ \text{fps}$
assumes $f:f \longrightarrow x$ **and** $g:g \longrightarrow y$
shows $((\lambda x. f\ x + g\ x) \longrightarrow x + y)$
<proof>

lemma *LIMSEQ-cmult-fps*:
fixes $x\ y :: 'a::\text{idom}\ \text{fps}$
assumes $f:f \longrightarrow x$
shows $((\lambda x. c * f\ x) \longrightarrow c * x)$
<proof>

6.3 The Hilbert Basis theorem

theorem *Hilbert-basis-FPS*:
assumes $h2:\langle \text{noetherian-ring } R \rangle$
shows $\langle \text{noetherian-ring FPS-ring} \rangle$
<proof>

end

end

7 The Real Ring definition

theory *Real-Ring-Definition*

```

imports
  HOL-Algebra.Module
  HOL-Algebra.RingHom
  HOL.Real
  HOL-Computational-Algebra.Formal-Power-Series
begin

Defining real ring for examples on Noetherian Rings.

definition
  REAL :: real ring
  where REAL = ( $\lambda$ carrier = UNIV, monoid.mult = (*), one = 1, zero = 0, add
    = (+))

lemma REAL-ring:  $\langle$ ring REAL $\rangle$ 
   $\langle$ proof $\rangle$ 

lemma REAL-crings:  $\langle$ cring REAL $\rangle$ 
   $\langle$ proof $\rangle$ 

lemma REAL-field:  $\langle$ field REAL $\rangle$ 
   $\langle$ proof $\rangle$ 

end

```

8 Examples

theory Examples-Noetherian-Rings

```

imports
  Hilbert-Basis
  Real-Ring-Definition
begin

```

8.1 Examples of noetherian rings with $\mathbb{Z}$ and $\mathbb{Z}[X]$

```

lemma INTEG-euclidean-domain:  $\langle$ euclidean-domain INTEG ( $\lambda x.$  nat (abs x)) $\rangle$ 
   $\langle$ proof $\rangle$ 

```

```

lemma principal-ideal-INTEG:  $\langle$ ideal I INTEG  $\implies$  principalideal I INTEG $\rangle$ 
   $\langle$ proof $\rangle$ 

```

```

lemma INTEG-noetherian-ring:  $\langle$ noetherian-ring INTEG $\rangle$ 
   $\langle$ proof $\rangle$ 

```

```

lemma INTEG-noetherian-domain:  $\langle$ noetherian-domain INTEG $\rangle$ 
   $\langle$ proof $\rangle$ 

```

lemma *Polynomials-INTEG-noetherian-ring*: $\langle$ noetherian-ring (univ-poly INTEG (carrier INTEG)) $\rangle$
 $\langle$ proof $\rangle$

lemma *Polynomials-INTEG-noetherian-domain*: $\langle$ noetherian-domain (univ-poly INTEG (carrier INTEG)) $\rangle$
 $\langle$ proof $\rangle$

8.2 Another example with $\mathbb{R}$ and $\mathbb{R}[X]$

lemma *REAL-noetherian-domain*: $\langle$ noetherian-domain REAL $\rangle$
 $\langle$ proof $\rangle$

lemma *PolyREAL-noetherian-domain*: $\langle$ noetherian-domain (univ-poly REAL (carrier REAL)) $\rangle$
 $\langle$ proof $\rangle$

end

References

- [1] Aaron Crighton *p-adic Fields and p-adic Semialgebraic Sets* , Archive of Formal Proofs, September 2022 https://www.isa-afp.org/entries/Padic_Field.html
- [2] Stack project <https://stacks.math.columbia.edu/tag/00FM>.
- [3] Vincent Douce <https://agreg-maths.fr/uploads/versions/1458/preview.pdf>.
- [4] Wiedijk's catalogue "Formalizing 100 Theorems" <https://www.cs.ru.nl/~freek/100/>, It appears at position 121 ...