Hilbert Basis Theorems*

Benjamin Puyobro

Benoît Ballenghien

Burkhart Wolff

Université Paris Saclay, IRT SystemX, LMF, CNRS

March 17, 2025

Contents

*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.

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.
- **Corrollary**. $\mathfrak{R}[X_1,...,X_n]$ 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*: ‹*ideal I R* ⟹ *carrier* (*R Quot I*) = {{*y*⊕*x* | *y*. *y*∈*I*} |*x*. *x*∈*carrier R*}›
⟨*proof*⟩

context
fixes *A B h*
assumes *ring-A*: ‹*ring A*›
assumes *ring-B*: ‹*ring B*›
assumes *h1*:‹*h*∈*ring-iso A B*›
begin
interpretation *ringA*: *ring A*
⟨*proof*⟩
interpretation *ringB*: *ring B*
⟨*proof*⟩

interpretation *rhr*:*ring-hom-ring A B h*
⟨*proof*⟩

lemma *inv-img-exist*:‹∀ *xa*∈*carrier B*. ∃ *y*. *y* ∈ *carrier A* ∧ *h y* = *xa*›
⟨*proof*⟩

lemma *img-ideal-is-ideal*:**assumes** *j1*:‹*ideal I A*›
shows ‹*ideal* (*h* ‘ *I*) *B*›
⟨*proof*⟩

lemma *img-in-carrier-quot*:‹∀ *x*∈ *carrier* (*A Quot I*). *h* ‘ *x* ∈ *carrier* (*B Quot* (*h*‘*I*))› **if** *j*:‹*ideal I A*› **for** *I*
⟨*proof*⟩

lemma *f8*:‹*xa*∈*carrier B* ∧ *xb*∈*I* ⟹*h*(*xb* $\oplus_A$ *inv-into* (*carrier A*) *h xa*) = *h xb* $\oplus_B$ *xa*› **if** *j*:‹*ideal I A*› **for** *I xb xa*
⟨*proof*⟩

lemma *f9*:‹∀ *xa*∈*carrier B*. ∀ *xb*∈*carrier A*. ∃ *y*. *h y* = *h xb* $\oplus_B$ *xa*›
⟨*proof*⟩

lemma *img-over-set-is-iso*: ‹*ideal I A* ⟹ ((‘) *h*) ∈ *ring-iso* (*A Quot I*) (*B Quot* (*h*‘*I*))› **for** *I*
⟨*proof*⟩
end

lemma *Quot-iso-cgen*:‹*a*∈*carrier A* ∧ *b*:*carrier B* ∧ *cring A* ∧ *cring B* ∧ *h* ∈ *ring-iso A B* ∧ *h*(*a*) = *b*
⟹ *A Quot* (*cgenideal A a*) ≃ *B Quot* (*cgenideal B b*)›
⟨*proof*⟩

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*:‹*deg-poly-set S k* = {*a*. *a*∈*S* ∧ *degree a* = *k*}∪{[]}›

definition (**in** *ring*) *lead-coeff-set*::‹′*a list set*⇒ *nat* ⇒ ′*a set*›
where ‹*lead-coeff-set S k* ≡ {*coeff a* (*degree a*) | *a*. *a*∈*deg-poly-set S k*}›

lemma *rule-union*:‹*x*∈(⋃ *n*≤*k*. *A l n*) ⟷ (∃ *n*≤*k*. *x*∈*A l n*)›
⟨*proof*⟩

lemma (**in** *ring*) *add-0-eq-0-is-0*:‹*a*∈*carrier* ((*carrier R*)[*X*]) ⟹ [] $\oplus_{(carrier\ R)\ [X]}$ *a* = [] ⟹ *a* = []›
⟨*proof*⟩

lemma (**in** *domain*) *inv-coeff-sum*:‹*a*∈*carrier*((*carrier R*)[*X*]) ⟹ *aa*∈*carrier*((*carrier R*)[*X*])
⟹ *a* $\oplus_{(carrier\ R)[X]}$ *aa* = [] ⟷ (∀ *n*. *coeff a n* = $inv_{add\text{-}monoid\ R}$ (*coeff aa n*))›
⟨*proof*⟩

lemma (**in** *ring*) *coeffs-of-add-poly*:‹*a*∈*carrier*((*carrier R*)[*X*]) ⟹ *aa*∈*carrier*((*carrier R*)[*X*])
⟹ *coeff* (*a* $\oplus_{(carrier\ R)[X]}$ *aa*) *n* = *coeff a n* ⊕ *coeff aa n*›

⟨*proof*⟩

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

lemma (**in** *domain*) *inv-imp-zero*:‹$a\in carrier((carrier\ R)[X]) \Longrightarrow a \oplus_{(carrier\ R)\ [X]}\ inv_{add\text{-}monoid\ ((carrier\ R)\ [X])}\ a = []$›
⟨*proof*⟩

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

lemma (**in** *domain*) *lead-coeff-in-carrier*:
‹$ideal\ I\ ((carrier\ R)[X]) \Longrightarrow a\in\ I \Longrightarrow coeff\ a\ (degree\ a) \in (carrier\ R)$› **for** I a
⟨*proof*⟩

lemma (**in** *domain*) *degree-of-inv*:‹$p\in carrier((carrier\ R)[X]) \Longrightarrow degree\ (inv_{add\text{-}monoid\ ((carrier\ R)[X])}\ p) = degree\ p$› **for** p
⟨*proof*⟩

lemma (**in** *domain*) *inv-in-deg-poly-set*:‹$ideal\ I\ ((carrier\ R)[X]) \Longrightarrow a\in\ deg\text{-}poly\text{-}set\ I\ k$
$\Longrightarrow inv_{add\text{-}monoid\ ((carrier\ R)[X])}\ a \in deg\text{-}poly\text{-}set\ I\ k$› **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*:‹$deg\text{-}poly\text{-}set\ x'\ 0 = \{[a] \mid a.\ [a]\in x'\}\cup\{[]\}$› **for** x'::‹$'c\ list\ set$›
⟨*proof*⟩

lemma (**in** *ring*) *lead-coeff-set-0*:‹$lead\text{-}coeff\text{-}set\ x'\ 0 = \{a.\ [a]\in x'\}\cup\{\mathbf{0}\}$› **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 card = 1) models of polynomials that exists in HOL-Algebra

4.1 Weak Hilbert Basis

lemma (**in** *noetherian-domain*) *weak-Hilbert-basis*:‹*noetherian-ring* ((*carrier R*)[*X*])›
⟨*proof*⟩

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*:‹*noetherian-ring A*› **and** *h2*:‹*ideal I A*›
shows‹*noetherian-ring* (*A Quot I*)›
⟨*proof*⟩

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

lemma *noetherian-isom-imp-noetherian*:
assumes *h1*:‹*noetherian-ring A* ∧ *ring B* ∧ $A \simeq B$›
shows ‹*noetherian-ring B*›
⟨*proof*⟩

lemma (**in** *domain*) *subring*:‹*subring* (*carrier R*) *R*›
⟨*proof*⟩

4.3 Some properties of the polynomial rings regarding ideals and quotients

lemma (**in** *domain*) *gen-is-cgen*:‹(*genideal* ((*carrier R*)[*X*]) {*X*}) = *cgenideal* ((*carrier R*)[*X*]) *X*›
⟨*proof*⟩

lemma (**in** *domain*) *principal-X*:‹*principalideal* (*genideal* ((*carrier R*)[*X*]) {*X*}) ((*carrier R*)[*X*])›
⟨*proof*⟩

named-theorems *poly*

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

‹(*cgenideal* ((*carrier R*)[*X*]) *X*) = {$a\otimes_{(carrier\ R)\ [X]}X$ |*a*. *a*∈*carrier*((*carrier R*)[*X*])}›
⟨*proof*⟩

lemma (**in** *domain*) *Idl-X*[*poly*]:
‹(*genideal* ((*carrier R*)[*X*]) {*X*})= {$a\otimes_{(carrier\ R)\ [X]}X$ |*a*. *a*∈*carrier*((*carrier R*)[*X*])}›
⟨*proof*⟩
lemma (**in** *domain*) *Idl-X-is-X*[*poly*]:
‹*p*∈(*genideal* ((*carrier R*)[*X*]) {*X*}) ⟹ ∃ *a*∈*carrier*((*carrier R*)[*X*]). $p = a\otimes_{(carrier\ R)\ [X]}X$
›
⟨*proof*⟩

lemma (**in** *ring*) *degree-of-nonempty-p*[*poly*]:‹*a*∈*carrier*((*carrier R*)[*X*]) ∧ *a*≠[] ⟹ *coeff a* (*degree a*) ≠ **0**›
⟨*proof*⟩

lemma (**in** *domain*)*coeff-0-of-mult-X*[*poly*]:‹*a*∈*carrier*((*carrier R*)[*X*]) ⟹ *coeff* ($a\otimes_{(carrier\ R)\ [X]}X$) *0* = **0**›
⟨*proof*⟩

lemma (**in** *domain*)*zero-coeff-of-Idl-X*[*poly*]:‹*p*∈*genideal* ((*carrier R*)[*X*]) {*X*} ⟹ *coeff p 0* = **0**›
⟨*proof*⟩

lemma (**in** *domain*) *mult-X-append-0*[*poly*]:‹*p*∈*carrier*((*carrier R*)[*X*]) ⟹ *p*≠[] ⟹ *poly-mult p X* = *p*@[**0**]›
⟨*proof*⟩

lemma (**in** *ring*) *polynomial-incl′*:‹*p*∈*carrier*((*carrier R*)[*X*]) ⟹ *set p* ⊆(*carrier R*)› **for** *p*
⟨*proof*⟩

lemma (**in** *ring*) *hd-in-carrier*:‹*p*≠ [] ⟹ *p*∈*carrier*((*carrier R*)[*X*]) ⟹ *hd p* ∈(*carrier R*)› **for** *p*
⟨*proof*⟩

lemma (**in** *ring*) *inv-in-carrier*:
‹*p*≠[] ⟹ *p*∈*carrier*((*carrier R*)[*X*]) ⟹ ($inv_{add\text{-}monoid\ R}$ (*hd p*)) ∈(*carrier R*)›
for *p*
⟨*proof*⟩

lemma (**in** *ring*) *inv-ld-coeff*:
‹*p*≠[] ⟹ *p*∈*carrier*((*carrier R*)[*X*]) ⟹ ($inv_{add\text{-}monoid\ R}$ (*hd p*)#*replicate* (*degree p*) **0**)∈*carrier*((*carrier R*)[*X*])›
for *p*
⟨*proof*⟩

lemma (**in** *ring*) *take-in-RX*:‹$p \in carrier((carrier\ R)[X]) \Longrightarrow n \leq length\ p \Longrightarrow (set\ (take\ n\ p)) \subseteq (carrier\ R)$› **for** *p n*
⟨*proof*⟩

lemma (**in** *ring*) *normalize-take-is-poly*:
‹$p \in carrier((carrier\ R)[X]) \Longrightarrow n \leq length\ p \Longrightarrow normalize\ (take\ n\ p) \in carrier((carrier\ R)[X])$› **for** *n p*
⟨*proof*⟩

lemma (**in** *ring*) *normalize-take-is-take*:‹$p \in carrier((carrier\ R)[X]) \wedge n \leq length\ p \Longrightarrow normalize\ (take\ n\ p) = take\ n\ p$›
⟨*proof*⟩

lemma (**in** *ring*) *take-in-carrier*:‹$p \in carrier((carrier\ R)[X]) \Longrightarrow n \leq length\ p \Longrightarrow (take\ n\ p) \in carrier((carrier\ R)[X])$›
⟨*proof*⟩

lemma (**in** *domain*) *take-misc-poly*:‹$p \in carrier((carrier\ R)[X]) \Longrightarrow p \neq [] \Longrightarrow coeff\ p\ 0 = \mathbf{0} \Longrightarrow ((take\ (degree\ p)\ p)) \otimes_{(carrier\ R)\ [X]} X = p$› **for** *p*
⟨*proof*⟩

lemma (**in** *ring*) *length-geq-2*:‹$normalize\ p \neq [] \wedge \neg(\exists\ a.\ normalize\ p = [a]) \Longrightarrow length\ p \geq 2$› **for** *p*::‹*'a list*›
⟨*proof*⟩

lemma (**in** *ring*) *norm-take-not-mt*:‹$length\ (normalize\ p) \geq 2 \Longrightarrow normalize\ (take\ (degree\ p)\ p) \neq []$› **for** *p*::‹*'a list*›
⟨*proof*⟩

lemma (**in** *ring*) *normalize-take-invariant*:‹$p \in carrier((carrier\ R)[X]) \Longrightarrow p \neq [] \Longrightarrow (normalize\ (take\ (degree\ p)\ p))@[coeff\ p\ 0] = p$›
for *p*
⟨*proof*⟩

lemma (**in** *domain*) *lower-coeff-add*:‹$p \neq [] \Longrightarrow p \in carrier((carrier\ R)[X]) \wedge b \in (carrier\ R)$
$\Longrightarrow coeff\ (((normalize\ p)\ @[\mathbf{0}]) \oplus_{(carrier\ R)\ [X]} [b]) = coeff\ ((normalize\ p)\ @[b])$›
for *p b*
⟨*proof*⟩

lemma (**in** *ring*) *cons-in-RX*:‹$a@p \in carrier((carrier\ R)[X]) \Longrightarrow normalize\ p \in carrier((carrier\ R)[X])$›
⟨*proof*⟩

lemma (**in** *ring*) *p-in-norm*:‹$p \in carrier((carrier\ R)[X]) \Longrightarrow normalize\ p = p$›
⟨*proof*⟩

lemma (**in** *domain*) *lower-coeff-add'*:‹$p \neq [] \Longrightarrow p \in carrier((carrier\ R)[X]) \wedge b \in$

(*carrier R*) ⟹ (((*normalize p*) @[**0**])$\oplus_{(carrier\ R)\ [X]}$ [*b*]) = ((*normalize p*) @[*b*])›
for *p b*
⟨*proof*⟩

lemma (**in** *domain*) *poly-invariant*:‹*p*∈*carrier*((*carrier R*)[*X*]) ⟹ *p*≠[] ⟹ ((*normalize* (*take* (*degree p*) *p*))$\otimes_{(carrier\ R)\ [X]}$*X*) $\oplus_{(carrier\ R)\ [X]}$ [*coeff p 0*] = *p*›
for *p*
⟨*proof*⟩

lemma (**in** *domain*) *gen-ideal-X-iff*:‹*p*∈(*genideal* ((*carrier R*)[*X*]) {*X*}) ⟷ (*p*∈*carrier* ((*carrier R*)[*X*]) ∧ *coeff p 0* = **0**)› **for** *p*::‹'*a list*›
⟨*proof*⟩

lemma (**in** *domain*) *gen-ideal-X-iff'*:‹(*genideal* ((*carrier R*)[*X*]) {*X*}) = {*p*∈*carrier* ((*carrier R*)[*X*]). *coeff p 0* = **0**}› **for** *p*::‹'*a list*›
⟨*proof*⟩

lemma (**in** *domain*) *quot-X-is-R*:‹*carrier* (((*carrier R*)[*X*]) *Quot* (*genideal* ((*carrier R*)[*X*]) {*X*}))
= {{*x*∈*carrier*((*carrier R*)[*X*]). *coeff x 0* = *a*} |*a*. *a*∈(*carrier R*)}›
⟨*proof*⟩

lemma (**in** *domain*) *uniq-a-quot*:
‹*c*∈ *carrier* (((*carrier R*)[*X*]) *Quot* (*genideal* ((*carrier R*)[*X*]) {*X*})) ⟹ ∃!*a*∈(*carrier R*). ∀ *y*∈*c*. *coeff y 0* = *a*›
⟨*proof*⟩

lemma (**in** *ring*) *append-in-carrier*:‹*a*∈*carrier*((*carrier R*)[*X*]) ∧ *b*∈*carrier*((*carrier R*)[*X*]) ⟹ *a*@*b* ∈ *carrier*((*carrier R*)[*X*])›
⟨*proof*⟩

lemma (**in** *domain*) *The-a-is-a*:‹*a*∈(*carrier R*) ⟹
(*THE aa*. ∀ *y*∈{*x* |*x*. *x* ∈ *carrier* ((*carrier R*) [*X*]) ∧ *local.coeff x 0* = *a*}. *local.coeff y 0* = *aa*) = *a*›
⟨*proof*⟩

lemma (**in** *ring*) *poly-mult-in-carrier2*:
⟦ *set p1* ⊆ *carrier R*; *set p2* ⊆ *carrier R* ⟧ ⟹ *poly-mult p1 p2* ∈ *carrier* ((*carrier R*)[*X*])
⟨*proof*⟩

lemma (**in** *ring*) *normalize-equiv*:‹*polynomial* (*carrier R*) (*normalize p*) ⟷ (*coeff* (*normalize p*)) ∈ *carrier* (*UP R*)›
⟨*proof*⟩

lemma (**in** *ring*) *p-in-RX-imp-in-P*:‹*p*∈*carrier* ((*carrier R*)[*X*]) ⟹ *coeff p* ∈ *up R*›
⟨*proof*⟩

lemma (**in** *ring*) *X-has-correp*:‹*coeff X* = (λ*i*. *if i* = *1 then* **1** *else* **0**)›
⟨*proof*⟩

lemma (**in** *ring*) *mult-is-mult*:
‹{*x*,*y*}⊆*carrier* ((*carrier R*)[*X*]) ⟹ *coeff* ($x \otimes_{(carrier\ R)[X]} y$) = *coeff x* $\otimes_{UP\ R}$ *coeff y*›
⟨*proof*⟩

lemma (**in** *ring*) *add-is-add*:‹*x* ∈ *carrier* (*poly-ring R*) ⟹
y ∈ *carrier* (*poly-ring R*)
⟹ *coeff* ($x \oplus_{poly\text{-}ring\ R} y$) = *coeff x* $\oplus_{UP\ R}$ *coeff y*›
⟨*proof*⟩

4.4 The isomorphisms between the different models of polynomials

lemma (**in** *ring*) *coeff-iso-RX-P*:‹*coeff* ∈ *ring-iso* (*poly-ring R*) (*UP R*)›
⟨*proof*⟩

lemma (**in** *ring*) *RX-iso-P*:‹(*carrier R*)[*X*] ≃ (*UP R*)›
⟨*proof*⟩

lemma (**in** *domain*) *R-isom-RX-X*:‹*R* ≃ (((*carrier R*)[*X*]) *Quot* (*genideal* ((*carrier R*)[*X*]) {*X*}))›
⟨*proof*⟩

lemma (**in** *domain*) *RX-imp-RX-over-X*:
‹*noetherian-ring* (*carrier R*[*X*]) ⟹ *noetherian-ring* (*carrier R*[*X*] *Quot* *genideal* (*carrier R*[*X*]) {*X*})›
⟨*proof*⟩

lemma (**in** *domain*) *noetherian-RX-imp-noetherian-R*:
‹*noetherian-ring* ((*carrier R*)[*X*]) ⟹ *noetherian-ring R*›
⟨*proof*⟩

lemma *principal-imp-noetherian*:‹*principal-domain R* ⟹ *noetherian-ring R*›
⟨*proof*⟩

lemma (**in** *ring*) *coeff-iff-poly-carrier*:‹*x* ∈ *carrier* (*poly-ring R*) ⟹
y ∈ *carrier* (*poly-ring R*) ⟹ (*x*=*y*) ⟷ *coeff x* = *coeff y*›
⟨*proof*⟩

lemma *zero-is-zero*:‹$B = B(\!|zero := \mathbf{0}_B|\!)$›
⟨*proof*⟩

lemma *ring-iso-imp-iso*:‹$A{\simeq}B \Longrightarrow A{\cong}B$›
⟨*proof*⟩

lemma (**in** *ring*) *iso-imp-exist-0*:‹$R{\simeq}B \Longrightarrow \exists\, x.\ ring\ (B(\!|zero{:=}x|\!))$›
⟨*proof*⟩

lemma (**in** *domain*) *noetherian-R-imp-noetherian-UP-R*:
assumes *h1*:‹*noetherian-ring R*›
shows ‹*noetherian-ring* (*UP R*)›
⟨*proof*⟩

lemma (**in** *domain*) *noetheriandom-R-imp-noetheriandom-UP-R*:
assumes *h1*:‹*noetherian-domain R*›
shows ‹*noetherian-domain* (*UP R*)›
⟨*proof*⟩

lemma (**in** *cring*) *Pring-one-index-isom-P*:‹$(Pring\ R\ \{N\}) \simeq UP\ R$›
⟨*proof*⟩

lemma (**in** *cring*) *P-isom-Pring-one-index*: ‹$UP\ R \simeq (Pring\ R\ \{N\})$›
⟨*proof*⟩

lemma (**in** *domain*) *P-iso-RX*:‹ $UP\ R \simeq ((carrier\ R)[X])$›
⟨*proof*⟩

lemma (**in** *domain*) *IP-noeth-imp-R-noeth*:‹*noetherian-ring* (*Pring R* $\{a\}$) $\Longrightarrow$ *noetherian-ring R*›
⟨*proof*⟩

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

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 $f \in$ *ring-hom R S*
  assumes $g \in$ *ring-hom S R*
  assumes $\bigwedge x.\ x \in$ *carrier R* $\Longrightarrow g\ (f\ x) = x$
  assumes $\bigwedge x.\ x \in$ *carrier S* $\Longrightarrow f\ (g\ x) = x$
  shows $f \in$ *ring-iso R S*
    $g \in$ *ring-iso S R*
⟨*proof*⟩

lemma(**in** *cring*) *var-factor-inverse*:
  assumes $I = J0 \cup J1$
  assumes $J1 \subseteq I$
  assumes $J1 \cap J0 = \{\}$
  assumes $\psi 1 =$ (*var-factor-inv I J0 J1*)
  assumes $\psi 0 =$ (*var-factor I J0 J1*)
  assumes $P \in$ *carrier* (*Pring* (*Pring R J0*) *J1*)
  shows $\psi 0\ (\psi 1\ P) = P$
⟨*proof*⟩

lemma(**in** *cring*) *var-factor-iso*:
  assumes $I = J0 \cup J1$
  assumes $J1 \subseteq I$
  assumes $J1 \cap J0 = \{\}$
  assumes $\psi 1 =$ (*var-factor-inv I J0 J1*)
  assumes $\psi 0 =$ (*var-factor I J0 J1*)
  shows $\psi 0 \in$ *ring-iso* (*Pring R I*) (*Pring* (*Pring R J0*) *J1*)
    $\psi 1 \in$ *ring-iso* (*Pring* (*Pring R J0*) *J1*)(*Pring R I*)
⟨*proof*⟩

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

shows (*Pring* (*Pring R J0*) *J1*) ≃ (*Pring R I*) **and** (*Pring R I*) ≃ (*Pring* (*Pring R J0*) *J1*)
⟨*proof*⟩

5.2 Preliminaries lemmas

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

lemma (**in** *cring*) *R-isom-P-mt*:‹*R* ≃ *Pring R* {}›
⟨*proof*⟩

5.3 Hilbert Basis theorem

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

theorem (**in** *domain*) *Hilbert-basis*:
assumes *h1*:‹*noetherian-ring R*› **and** *h2*:‹*finite I*›
shows ‹*noetherian-ring* (*Pring R I*)›
⟨*proof*⟩

lemma (**in** *domain*) *R-noetherian-implies-IP-noetherian*:
assumes *h1*:‹*noetherian-ring R*›
shows ‹*noetherian-ring* (*Pring R* {*0..N::nat*})›
⟨*proof*⟩

lemma (**in** *domain*) *IP-noetherian-implies-R-noetherian*:
assumes *h1*:‹*noetherian-ring* (*Pring R I*)› **and** *h2*:‹*finite I*›
shows ‹*noetherian-ring R*›
⟨*proof*⟩

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*::‹*'a*::{*idom*} *ring*› (**structure**)
  defines *R*:‹*R* ≡ (|*carrier* = *UNIV*, *monoid.mult* = (∗), *one* = *1*, *zero* = *0*, *add* = (+)|)›
begin

lemma *ring-R*:‹*ring R*›
  ⟨*proof*⟩

lemma *domain-R*:‹*domain R*›
  ⟨*proof*⟩

definition
  FPS-ring :: *'a*::{*idom*} *fps ring*
  where *FPS-ring* = (|*carrier* = *UNIV*, *monoid.mult* = (∗), *one* = *1*, *zero* = *0*, *add* = (+)|)

lemma *ring-FPS*:‹*ring FPS-ring*›
  ⟨*proof*⟩

lemma *cring-FPS*:‹*cring FPS-ring*›
  ⟨*proof*⟩

lemma *domain-FPS*:‹*domain FPS-ring*›
  ⟨*proof*⟩

valuation over FPS_ring

definition *v-subdegree* :: (*'a*::{*idom*}) *fps* ⇒ *enat* **where**
  v-subdegree f = (*if f* = *0 then* ∞ *else subdegree f*)

definition *valuation*::‹*'a*::{*idom*} *fps* ⇒ *enat*› (*ν*)**where**
  ‹*ν x* ≡ *Sup* {*enat k* |*k*. *x*∈ *cgenideal FPS-ring* (*fps-X^k*)}›

lemma *fps-X-pow-k-ideal-iff*:‹*cgenideal FPS-ring* (*fps-X^k*) = {*x*. *v-subdegree x* ≥ *k*}›
⟨*proof*⟩

lemma *valuation-miscs-1*:**assumes** *h1*:‹*f* ∈*carrier FPS-ring*›
shows ‹(*valuation f*) = (∞::*enat*) ⟷ *f* = *0*›
⟨*proof*⟩

lemma *valuation-miscs-0*:
shows ‹*valuation f* = *Inf* {*enat n* |*n*. *fps-nth f n* ≠ *0*}›
⟨*proof*⟩

lemma *valuation-miscs-3*:‹*valuation f* = *v-subdegree f*›
⟨*proof*⟩

lemma *triangular-ineq-v*:‹*valuation* (*f* + *g*) ≥ *min* (*valuation f*) (*valuation g*)›
⟨*proof*⟩

lemma *triang-eq-v*:**assumes** *h1*:‹*valuation f*≠ *valuation g*›
shows ‹*valuation* (*f*+*g*) = *min* (*valuation f*) (*valuation g*)›
⟨*proof*⟩

lemma *prod-triang-v*:‹*valuation* (*f*∗*g*) = *valuation f* + *valuation g*›
⟨*proof*⟩

6.2 Premisses for noetherian ring proof

definition *subdeg-poly-set*:‹*subdeg-poly-set S k* = {*a*. *a*∈*S* ∧ *subdegree a* = *k*}∪{*0*}›

definition *sublead-coeff-set*::‹′*b*::{*zero*} *fps set*⇒ *nat* ⇒ ′*b set*›
where ‹*sublead-coeff-set S k* ≡ { *fps-nth a* (*subdegree a*) | *a*. *a*∈ *subdeg-poly-set S k*}›

lemma *ideal-nonempty*:‹*ideal I FPS-ring* ⟹ *I* ≠ {}›
⟨*proof*⟩

lemma *mult-X-in-ideal*:‹*ideal I FPS-ring* ⟹ ∀ *x*∈*I*. *fps-X* ∗ *x* ∈ *I*›
⟨*proof*⟩

lemma *non-empty-sublead*:‹*ideal I FPS-ring* ⟹ *sublead-coeff-set I k* ≠ {}›
⟨*proof*⟩

lemma *inv-unique*:‹∀ *x*∈*carrier FPS-ring*. ∃!*y*. *x* + *y* = *0*›
⟨*proof*⟩

lemma *inv-same-degree*:**assumes** *h*:‹*x*∈*carrier FPS-ring*›
shows‹*subdegree* ($inv_{add\text{-}monoid\ FPS\text{-}ring}$ *x*) = *subdegree x*›
⟨*proof*⟩

lemma *inv-subdegree-is-inv*: **assumes** *h*:*x*∈*carrier FPS-ring*
shows ‹*fps-nth* ($inv_{add\text{-}monoid\ FPS\text{-}ring}$ *x*) (*subdegree x*) =
($inv_{add\text{-}monoid\ R}$ (*fps-nth x* (*subdegree x*)))›

⟨proof⟩

lemma *subdeg-inv-in-sublead*:
assumes *h1*:‹*ideal I FPS-ring*› **and** *h2*:‹$a \in$ *sublead-coeff-set I k*›
shows ‹$inv_{add\text{-}monoid\ R}\ a \in$ *sublead-coeff-set I k*›
⟨proof⟩

lemma *mult-stable-sublead*:
assumes *h1*:‹*ideal I FPS-ring*›
and *h2*:‹$a \in$ *sublead-coeff-set I k*›
and *h3*:‹$b \in$ *sublead-coeff-set I k*›
shows ‹$a \otimes_R b \in$ *sublead-coeff-set I k*›
⟨proof⟩

lemma *add-stable-sublead*:
assumes *h1*:‹*ideal I FPS-ring*›
and *h2*:‹$a \in$ *sublead-coeff-set I k*›
and *h3*:‹$b \in$ *sublead-coeff-set I k*›
shows ‹$a \otimes_{add\text{-}monoid\ R} b \in$ *sublead-coeff-set I k*›
⟨proof⟩

lemma *outer-stable-sublead*:
assumes *h1*:‹*ideal I FPS-ring*›**and** *h2*:‹$a \in$ *sublead-coeff-set I k*› **and** *h3*:‹$b \in$ *carrier R*›
shows ‹$b \otimes a \in$ *sublead-coeff-set I k*›
⟨proof⟩

lemma *sublead-ideal*:‹*ideal I FPS-ring* $\Longrightarrow$ *ideal* (*sublead-coeff-set I k*) *R*›
⟨proof⟩

lemma *order-sublead*:
assumes *h1*:‹$J1 \subseteq J2$› **and** *h2*:‹*ideal J1 FPS-ring*› **and** *h3*:‹*ideal J2 FPS-ring*›
shows ‹*sublead-coeff-set J1 k* $\subseteq$ *sublead-coeff-set J2 k*›
⟨proof⟩

lemma *sup-sublead-stable-add*:‹*ideal I FPS-ring* $\Longrightarrow$
$a \in \bigcup$ (*range* (*sublead-coeff-set I*)) $\Longrightarrow$
$b \in \bigcup$ (*range* (*sublead-coeff-set I*))
$\Longrightarrow a \otimes_{add\text{-}monoid\ R} b \in \bigcup$ (*range* (*sublead-coeff-set I*))›
⟨proof⟩

lemma *sup-sublead-ideal*:‹*ideal I FPS-ring* $\Longrightarrow$ *ideal* ($\bigcup$ *k. sublead-coeff-set I k*) *R*›
⟨proof⟩

lemma *Sub-subdeg-eq-ideal*:‹*ideal J FPS-ring* $\Longrightarrow$ ($\bigcup$ *k. subdeg-poly-set J k*) = *J*›
⟨proof⟩

lemma *eq-subdeg*:
  assumes *h1*:‹*J1* ⊆ *J2*›
    and *h3*:‹ *ideal J1 FPS-ring*› **and** *h4*:‹*ideal J2 FPS-ring*›
  shows ‹*J1* = *J2* ⟷ (∀ *k*. *subdeg-poly-set J1 k* = *subdeg-poly-set J2 k*)›
⟨*proof*⟩

lemma *inculded-sublead*:‹*ideal I FPS-ring* ⟹ *sublead-coeff-set I k* ⊆ *sublead-coeff-set I* (*k*+*1*)›
  ⟨*proof*⟩

lemma *included-sublead-gen*:**assumes** ‹*ideal I FPS-ring*› ‹*k*≤*k*′›
  shows ‹*sublead-coeff-set I k* ⊆ *sublead-coeff-set I* (*k*′)›
  ⟨*proof*⟩

lemma *sup-sublead*:
  assumes *h1*:‹*ideal I FPS-ring*›
    and *h2*: ‹*noetherian-ring R*›
  shows ‹(⋃ {*sublead-coeff-set I k*|*k*. *k*∈*UNIV*}) ∈ {*sublead-coeff-set I k*|*k*. *k*∈*UNIV*}›
  ⟨*proof*⟩

lemma *subdeg-inf-imp-s-tendsto-zero*:
  fixes *s*::‹*nat* ⇒ ′*a*::{*idom*} *fps*›
  assumes *g2*:‹*strict-mono* (λ*n*. *subdegree* (*s n*))›
  shows ‹*s* ⟶ *0*›
⟨*proof*⟩

lemma *idl-sum*:‹*finite A* ⟹ *ideal* {*x*. ∃ *s*. *x*=(∑ *i*∈{*0*..<*card A*}. *s i* ∗ *from-nat-into A i*)} *R*› **for** *A*
⟨*proof*⟩

lemma *genideal-sum-rep*:
  ‹*finite A* ⟹ *genideal R A* = {*x*. ∃ *s*. *x*=(∑ *i*∈{*0*..<*card A*}. *s i* ∗ *from-nat-into A i*)}› **for** *A*
⟨*proof*⟩

lemma *fps-sum-rep-nth*′:
  fps-nth (*sum* (λ*i*. *fps-const*(*a i*)∗*fps-X*^*i*) {*0*..*m*}) *n* = (*if n* ≤ *m then a n else 0*)
  ⟨*proof*⟩

lemma *abs-tndsto*: **shows** ‹(λ*n*. (∑ *i*≤*n*. *fps-const* (*s i*) ∗ *fps-X*^*i*)::′*a fps*) ⟶ *Abs-fps s*›
  (**is** ‹*?s* ⟶ *?a*›)
⟨*proof*⟩

lemma *add-stable-FPS-ring*:‹*ideal I FPS-ring* $\Longrightarrow$ *a*∈*I* $\Longrightarrow$ *b*∈*I* $\Longrightarrow$ *a*+*b* ∈ *I*›
⟨*proof*⟩

lemma *abs-tndsto-le*: **shows** ‹(λ*n*. (∑ *i*<*n*. *fps-const* (*s i*) ∗ *fps-X*^*i*)::′*a fps*) ⟶ *Abs-fps s*›
⟨*proof*⟩

lemma *bij-betw-strict-mono*:
assumes ‹*strict-mono* (*f*::*nat*⇒*nat*)›
shows ‹*bij-betw f UNIV* (*f*‘*UNIV*)›
⟨*proof*⟩

lemma *no-i-inf-0*:‹*strict-mono* (*f*::*nat*⇒*nat*) $\Longrightarrow$ *i*<*f 0* $\Longrightarrow$ ¬(∃ *j*. *f j* = *i*)›
⟨*proof*⟩

lemma *inter-mt*:‹*strict-mono* (*f*::*nat*⇒*nat*) $\Longrightarrow$ {..<*f 0*} ∩ *range f* = {}›
⟨*proof*⟩

lemma *range-inter-f*:‹*strict-mono* (*f*::*nat*⇒*nat*) $\Longrightarrow$ {..<*f n*} ∩ *range f* = *f*‘{*0*..<*n*}›
⟨*proof*⟩

lemma *simp-rule-sum*:‹*strict-mono* (*f*::*nat*⇒*nat*) $\Longrightarrow$ (∑ *i*∈{..<*f* (*Suc n*)}. (*if i* ∈ *range f*
then (*s* ((*inv-into UNIV f*) *i*)) ∗*fps-X*^*i else 0*)) = (∑ *i*∈{..<*f n*}. (*if i* ∈ *range f then*
(*s* ((*inv-into UNIV f*) *i*)) ∗*fps-X*^*i else 0*)) + (*s* ((*inv-into UNIV f*) (*f n*))) ∗*fps-X*^(*f n*)›
⟨*proof*⟩

lemma *rewriting-sum*: **assumes** ‹*strict-mono* (*f*::*nat*⇒*nat*)›
shows ‹(∑ *i*<*n*. *fps-const* (*s i*) ∗ *fps-X*^(*f i*))
= (∑ *i*∈{..<*f n*}. (*if i* ∈ *range f then fps-const* (*s* (*inv-into UNIV f i*)) ∗*fps-X*^*i else 0*))›
⟨*proof*⟩

lemma *exists-seq*:‹*strict-mono* (*f*::*nat*⇒*nat*) $\Longrightarrow$
∃ *s*. (∑ *i*∈{..<*f n*}. (*if i* ∈ *range f then fps-const* (*s*′ (*inv-into UNIV f i*)) ∗*fps-X*^*i else 0*))
= (∑ *i*∈{..<*f n*}. *fps-const* (*s i*) ∗*fps-X*^*i*)›
⟨*proof*⟩

lemma *exists-seq*′:‹*strict-mono* (*f*::*nat*⇒*nat*) $\Longrightarrow$
∃ *s*. (∑ *i*<*n*. *fps-const* (*s*′ *i*) ∗ (*fps-X*::′*a fps*)^(*f i*)) =
(∑ *i*∈{..<*f n*}. *fps-const* (*s i*) ∗*fps-X*^*i*)›
⟨*proof*⟩

lemma *exists-seq-all*:‹*strict-mono* (*f*::*nat*⇒*nat*) ⟹
∃ *s*. ∀ *n*. (∑ *i*∈{..<*f n*}. (*if i* ∈ *range f then fps-const* (*s*′ (*inv-into UNIV f i*)) ∗*fps-X*^*i else 0*))
= (∑ *i*∈{..<*f n*}. *fps-const* (*s i*) ∗*fps-X*^*i*)›
⟨*proof*⟩

lemma *exists-seq-all*′:‹*strict-mono* (*f*::*nat*⇒*nat*) ⟹
∃ *s*. ∀ *n*. (∑ *i*<*n*. *fps-const* (*s*′ *i*) ∗ *fps-X*^(*f i*)) =
(∑ *i*∈{..<*f n*}. *fps-const* (*s i*) ∗*fps-X*^*i*)›
⟨*proof*⟩

lemma *tendsto-f-seq*:**assumes** ‹*strict-mono* (*f*::*nat*⇒*nat*)›
shows ‹(λ*n*. (∑ *i*∈{..<*f n*}. *fps-const* (*s i*) ∗*fps-X*^*i*)::′*a fps*) ⟶ *Abs-fps* (λ*i*. *s i*)›
⟨*proof*⟩

lemma *LIMSEQ-add-fps*:
fixes *x y* :: ′*a*::*idom fps*
assumes *f*:*f* ⟶ *x* **and** *g*:(*g* ⟶ *y*)
shows ((λ*x*. *f x* + *g x*) ⟶ *x* + *y*)
⟨*proof*⟩

lemma *LIMSEQ-cmult-fps*:
fixes *x y* :: ′*a*::*idom fps*
assumes *f*:*f* ⟶ *x*
shows ((λ*x*. *c* ∗ *f x*) ⟶ *c*∗*x*)
⟨*proof*⟩

6.3 The Hilbert Basis theorem

theorem *Hilbert-basis-FPS*:
assumes *h2*:‹*noetherian-ring R*›
shows ‹*noetherian-ring FPS-ring*›
⟨*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* = (|*carrier* = *UNIV*, *monoid.mult* = (∗), *one* = *1*, *zero* = *0*, *add* = (+)|)

lemma *REAL-ring*:‹*ring REAL*›
⟨*proof*⟩

lemma *REAL-cring*:‹*cring REAL*›
⟨*proof*⟩

lemma *REAL-field*: ‹*field REAL*›
⟨*proof*⟩

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*:‹*euclidean-domain INTEG* (λ*x*. *nat* (*abs x*))›
⟨*proof*⟩

lemma *principal-ideal-INTEG*:‹*ideal I INTEG* ⟹ *principalideal I INTEG*›
⟨*proof*⟩

lemma *INTEG-noetherian-ring*:‹*noetherian-ring INTEG*›
⟨*proof*⟩

lemma *INTEG-noetherian-domain*:‹*noetherian-domain INTEG*›
⟨*proof*⟩

lemma *Polynomials-INTEG-noetherian-ring*:‹*noetherian-ring* (*univ-poly INTEG* (*carrier INTEG*))›
⟨*proof*⟩

lemma *Polynomials-INTEG-noetherian-domain*: ‹*noetherian-domain* (*univ-poly INTEG* (*carrier INTEG*))›
⟨*proof*⟩

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

lemma *REAL-noetherian-domain*:‹*noetherian-domain REAL*›
⟨*proof*⟩

lemma *PolyREAL-noetherian-domain*:‹*noetherian-domain* (*univ-poly REAL* (*carrier REAL*))›
⟨*proof*⟩

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 ...