Fundamental Properties of Valuation Theory and Hensel's Lemma

Hidetsune Kobayashi

December 14, 2021

Abstract

Convergence with respect to a valuation is discussed as convergence of a Cauchy sequence. Cauchy sequences of polynomials are defined. They are used to formalize Hensel's lemma.

Contents

theory *Valuation1*
imports *Group−Ring−Module.Algebra9*
begin

declare *ex-image-cong-iff* [*simp del*]

Chapter 1

Preliminaries

1.1 Int and ant (augmented integers)

lemma *int-less-mono*:$(a::nat) < b \Longrightarrow int\ a < int\ b$
⟨*proof*⟩

lemma *zless-trans*:$[\![(i::int) < j;\ j < k]\!] \Longrightarrow i < k$
⟨*proof*⟩

lemma *zmult-pos-bignumTr0*:$\exists\, L.\ \forall\, m.\ L < m \longrightarrow z < x + int\ m$
⟨*proof*⟩

lemma *zle-less-trans*:$[\![(i::int) \leq j;\ j < k]\!] \Longrightarrow i < k$
⟨*proof*⟩

lemma *zless-le-trans*:$[\![(i::int) < j;\ j \leq k]\!] \Longrightarrow i < k$
⟨*proof*⟩

lemma *zmult-pos-bignumTr*:$0 < (a::int) \Longrightarrow$
$\exists\, l.\ \forall\, m.\ l < m \longrightarrow z < x + (int\ m) * a$
⟨*proof*⟩

lemma *ale-shift*:$[\![(x::ant) \leq y;\ y = z]\!] \Longrightarrow x \leq z$
⟨*proof*⟩

lemma *aneg-na-0*[*simp*]:$a < 0 \Longrightarrow na\ a = 0$
⟨*proof*⟩

lemma *amult-an-an*:$an\ (m * n) = (an\ m) * (an\ n)$
⟨*proof*⟩

definition
adiv :: [*ant*, *ant*] ⇒ *ant* (**infixl** *adiv 200*) **where**
x adiv y = *ant* ((*tna x*) *div* (*tna y*))

definition
amod :: [*ant*, *ant*] ⇒ *ant* (**infixl** *amod 200*) **where**
x amod y = *ant* ((*tna x*) *mod* (*tna y*))

lemma *apos-amod-conj*:*0* < *ant b* ⟹
0 ≤ (*ant a*) *amod* (*ant b*) ∧ (*ant a*) *amod* (*ant b*) < (*ant b*)
⟨*proof*⟩

lemma *amod-adiv-equality*:
(*ant a*) = (*a div b*) $*_a$ (*ant b*) + *ant* (*a mod b*)
⟨*proof*⟩

lemma *asp-z-Z*:*z* $*_a$ *ant x* ∈ Z_∞
⟨*proof*⟩

lemma *apos-in-aug-inf*:*0* ≤ *a* ⟹ *a* ∈ Z_∞
⟨*proof*⟩

lemma *amult-1-both*:⟦*0* < (*w*::*ant*); *x* ∗ *w* = *1*⟧ ⟹ *x* = *1* ∧ *w* = *1*
⟨*proof*⟩

lemma *poss-int-neq-0*:*0* < (*z*::*int*) ⟹ *z* ≠ *0*
⟨*proof*⟩

lemma *aadd-neg-negg*[*simp*]:⟦*a* ≤ (*0*::*ant*); *b* < *0*⟧ ⟹ *a* + *b* < *0*
⟨*proof*⟩

lemma *aadd-two-negg*[*simp*]:⟦*a* < (*0*::*ant*); *b* < *0*⟧ ⟹ *a* + *b* < *0*
⟨*proof*⟩

lemma *amin-aminTr*:(*z*::*ant*) ≤ *z'* ⟹ *amin z w* ≤ *amin z' w*
⟨*proof*⟩

lemma *amin-le1*:(*z*::*ant*) ≤ *z'* ⟹ (*amin z w*) ≤ *z'*
⟨*proof*⟩

lemma *amin-le2*:(*z*::*ant*) ≤ *z'* ⟹ (*amin w z*) ≤ *z'*
⟨*proof*⟩

lemma *Amin-geTr*:(∀ *j* ≤ *n*. *f j* ∈ Z_∞) ∧ (∀ *j* ≤ *n*. *z* ≤ (*f j*)) ⟶
z ≤ (*Amin n f*)
⟨*proof*⟩

lemma *Amin-ge*:⟦∀ *j* ≤ *n*. *f j* ∈ Z_∞; ∀ *j* ≤ *n*. *z* ≤ (*f j*)⟧ ⟹
z ≤ (*Amin n f*)
⟨*proof*⟩

definition
Abs :: *ant* ⇒ *ant* **where**

$Abs\ z = (if\ z < 0\ then\ -z\ else\ z)$

lemma *Abs-pos*:$0 \leq Abs\ z$
⟨*proof*⟩

lemma *Abs-x-plus-x-pos*:$0 \leq (Abs\ x) + x$
⟨*proof*⟩

lemma *Abs-ge-self*:$x \leq Abs\ x$
⟨*proof*⟩

lemma *na-1*:$na\ 1 = Suc\ 0$
⟨*proof*⟩

lemma *ant-int*:$ant\ (int\ n) = an\ n$
⟨*proof*⟩

lemma *int-nat*:$0 < z \Longrightarrow int\ (nat\ z) = z$
⟨*proof*⟩

lemma *int-ex-nat*:$0 < z \Longrightarrow \exists\, n.\ int\ n = z$
⟨*proof*⟩

lemma *eq-nat-pos-ints*:
$[\![nat\ (z::int) = nat\ (z'::int);\ 0 \leq z;\ 0 \leq z']\!] \Longrightarrow z = z'$
⟨*proof*⟩

lemma *a-p1-gt*[*simp*]:$[\![a \neq \infty;\ a \neq -\infty]\!] \Longrightarrow a < a + 1$
⟨*proof*⟩

lemma *gt-na-poss*:$(na\ a) < m \Longrightarrow 0 < m$
⟨*proof*⟩

lemma *azmult-less*:$[\![a \neq \infty;\ na\ a < m;\ 0 < x]\!]$
$\Longrightarrow a < int\ m *_a x$
⟨*proof*⟩

lemma *zmult-gt-one*:$[\![2 \leq m;\ 0 < xa]\!] \Longrightarrow 1 < int\ m * xa$
⟨*proof*⟩

lemma *zmult-pos*:$[\![\ 0 < m;\ 0 < (a::int)]\!] \Longrightarrow 0 < (int\ m) * a$
⟨*proof*⟩

lemma *ant-int-na*:$[\![0 \leq a;\ a \neq \infty\ ]\!] \Longrightarrow ant\ (int\ (na\ a)) = a$
⟨*proof*⟩

lemma *zpos-nat*:$0 \leq (z::int) \Longrightarrow \exists\, n.\ z = int\ n$
⟨*proof*⟩

1.2 nsets

lemma *nsetTr1*:$[\![j \in nset\ a\ b;\ j \neq a]\!] \Longrightarrow j \in nset\ (Suc\ a)\ b$
⟨*proof*⟩

lemma *nsetTr2*:$j \in nset\ (Suc\ a)\ (Suc\ b) \Longrightarrow j - Suc\ 0 \in nset\ a\ b$
⟨*proof*⟩

lemma *nsetTr3*:$[\![j \neq Suc\ (Suc\ 0);\ j - Suc\ 0 \in nset\ (Suc\ 0)\ (Suc\ n)]\!]$
$\Longrightarrow\ Suc\ 0 < j - Suc\ 0$
⟨*proof*⟩

lemma *Suc-leD1*:$Suc\ m \leq n \Longrightarrow m < n$
⟨*proof*⟩

lemma *leI1*:$n < m \Longrightarrow \neg\ ((m::nat) \leq n)$
⟨*proof*⟩

lemma *neg-zle*:$\neg\ (z::int) \leq z' \Longrightarrow z' < z$
⟨*proof*⟩

lemma *nset-m-m*:$nset\ m\ m = \{m\}$
⟨*proof*⟩

lemma *nset-Tr51*:$[\![j \in nset\ (Suc\ 0)\ (Suc\ (Suc\ n));\ j \neq Suc\ 0]\!]$
$\Longrightarrow j - Suc\ 0 \in nset\ (Suc\ 0)\ (Suc\ n)$
⟨*proof*⟩

lemma *nset-Tr52*:$[\![j \neq Suc\ (Suc\ 0);\ Suc\ 0 \leq j - Suc\ 0]\!]$
$\Longrightarrow \neg\ j - Suc\ 0 \leq Suc\ 0$
⟨*proof*⟩

lemma *nset-Suc*:$nset\ (Suc\ 0)\ (Suc\ (Suc\ n)) =$
$nset\ (Suc\ 0)\ (Suc\ n) \cup \{Suc\ (Suc\ n)\}$
⟨*proof*⟩

lemma *AinequalityTr0*:$x \neq -\infty \Longrightarrow \exists\, L.\ (\forall\, N.\ L < N \longrightarrow$
$(an\ m) < (x + an\ N))$
⟨*proof*⟩

lemma *AinequalityTr*:$[\![0 < b \wedge b \neq \infty;\ x \neq -\infty]\!] \Longrightarrow \exists\, L.\ (\forall\, N.\ L < N \longrightarrow$
$(an\ m) < (x + (int\ N) *_a b))$
⟨*proof*⟩

lemma *two-inequalities*:$[\![\forall\, (n::nat).\ x < n \longrightarrow P\ n;\ \forall\, (n::nat).\ y < n \longrightarrow Q\ n]\!]$
$\Longrightarrow\ \forall\, n.\ (max\ x\ y) < n \longrightarrow (P\ n) \wedge (Q\ n)$
⟨*proof*⟩

lemma *multi-inequalityTr0*:$(\forall\, j \leq (n::nat).\ (x\ j) \neq -\infty\ ) \longrightarrow$

$(\exists\, L.\ (\forall\, N.\ L < N \longrightarrow\ (\forall\, l \leq n.\ (an\ m) < (x\ l) + (an\ N))))$
⟨*proof*⟩

lemma *multi-inequalityTr1*:$[\![\forall\, j \leq (n::nat).\ (x\ j) \neq -\infty]\!] \Longrightarrow$
$\exists\, L.\ (\forall\, N.\ L < N \longrightarrow\ (\forall\, l \leq n.\ (an\ m) < (x\ l) + (an\ N)))$
⟨*proof*⟩

lemma *gcoeff-multi-inequality*:$[\![\forall\, N.\ 0 < N \longrightarrow (\forall\, j \leq (n::nat).\ (x\ j) \neq -\infty \wedge$
$0 < (b\ N\ j) \wedge (b\ N\ j) \neq \infty)]\!] \Longrightarrow$
$\exists\, L.\ (\forall\, N.\ L < N \longrightarrow\ (\forall\, l \leq n.(an\ m) < (x\ l) + (int\ N) *_a (b\ N\ l)))$
⟨*proof*⟩

primrec *m-max* :: $[nat,\ nat \Rightarrow nat] \Rightarrow nat$
where
m-max-0: *m-max 0 f* = *f 0*
| *m-max-Suc*: *m-max* (*Suc n*) *f* = *max* (*m-max n f*) (*f* (*Suc n*))

lemma *m-maxTr*:$\forall\, l \leq n.\ (f\ l) \leq$ *m-max n f*
⟨*proof*⟩

lemma *m-max-gt*:$l \leq n \Longrightarrow (f\ l) \leq$ *m-max n f*
⟨*proof*⟩

lemma *ASum-zero*: $(\forall\, j \leq n.\ f\ j \in Z_\infty) \wedge (\forall\, l \leq n.\ f\ l = 0) \longrightarrow ASum\ f\ n = 0$
⟨*proof*⟩

lemma *eSum-singleTr*:$(\forall\, j \leq n.\ f\ j \in Z_\infty) \wedge (j \leq n \wedge (\forall\, l \in \{h.\ h \leq n\} - \{j\}.\ f\ l$
$= 0)) \longrightarrow ASum\ f\ n = f\ j$
⟨*proof*⟩

lemma *eSum-single*:$[\![\forall\, j \leq n.\ f\ j \in Z_\infty\ ;\ j \leq n;\ \forall\, l \in \{h.\ h \leq n\} - \{j\}.\ f\ l = 0]\!]$
$\Longrightarrow ASum\ \ f\ n = f\ j$
⟨*proof*⟩

lemma *ASum-eqTr*:$(\forall\, j \leq n.\ f\ j \in Z_\infty) \wedge (\forall\, j \leq n.\ g\ j \in Z_\infty) \wedge$
$(\forall\, j \leq n.\ f\ j = g\ j) \longrightarrow ASum\ f\ n = ASum\ g\ n$
⟨*proof*⟩

lemma *ASum-eq*:$[\![\forall\, j \leq n.\ f\ j \in Z_\infty;\ \forall\, j \leq n.\ g\ j \in Z_\infty;\ \forall\, j \leq n.\ f\ j = g\ j]\!] \Longrightarrow$
$ASum\ f\ n = ASum\ g\ n$
⟨*proof*⟩

definition
Kronecker-delta :: $[nat,\ nat] \Rightarrow ant$
((*δ*_ _) [*70*,*71*]*70*) **where**
$\delta_{i\ j}$ = (*if i* = *j then 1 else 0*)

definition
K-gamma :: [*nat*, *nat*] ⇒ *int*
((γ_ _) [70,71]70) **where**
$\gamma_{i\,j} = (\mathit{if}\ i = j\ \mathit{then}\ 0\ \mathit{else}\ 1)$

abbreviation
TRANSPOS ((τ_ _) [90,91]90) **where**
$\tau_{i\,j} == \mathit{transpos}\ i\ j$

lemma *Kdelta-in-Zinf*:⟦$j \leq (\mathit{Suc}\ n)$; $k \leq (\mathit{Suc}\ n)$⟧ ⟹
$z *_a (\delta_{j\,k}) \in Z_\infty$
⟨*proof*⟩

lemma *Kdelta-in-Zinf1*:⟦$j \leq n$; $k \leq n$⟧ ⟹ $\delta_{j\,k} \in Z_\infty$
⟨*proof*⟩

primrec *m-zmax* :: [*nat*, *nat* ⇒ *int*] ⇒ *int*
where
m-zmax-0: $\mathit{m\text{-}zmax}\ 0\ f = f\ 0$
| *m-zmax-Suc*: $\mathit{m\text{-}zmax}\ (\mathit{Suc}\ n)\ f = \mathit{zmax}\ (\mathit{m\text{-}zmax}\ n\ f)\ (f\ (\mathit{Suc}\ n))$

lemma *m-zmax-gt-eachTr*:
$(\forall j \leq n.\ f\,j \in \mathit{Zset}) \longrightarrow (\forall j \leq n.\ (f\,j) \leq \mathit{m\text{-}zmax}\ n\ f)$
⟨*proof*⟩

lemma *m-zmax-gt-each*:$(\forall j \leq n.\ f\,j \in \mathit{Zset}) \Longrightarrow (\forall j \leq n.\ (f\,j) \leq \mathit{m\text{-}zmax}\ n\ f)$
⟨*proof*⟩

lemma *n-notin-Nset-pred*: $0 < n \Longrightarrow \neg\ n \leq (n - \mathit{Suc}\ 0)$
⟨*proof*⟩

lemma *Nset-preTr*:⟦$0 < n$; $j \leq (n - \mathit{Suc}\ 0)$⟧ ⟹ $j \leq n$
⟨*proof*⟩

lemma *Nset-preTr1*:⟦$0 < n$; $j \leq (n - \mathit{Suc}\ 0)$⟧ ⟹ $j \neq n$
⟨*proof*⟩

lemma *transpos-noteqTr*:⟦$0 < n$; $k \leq (n - \mathit{Suc}\ 0)$; $j \leq n$; $j \neq n$⟧
⟹ $j \neq (\tau_{j\,n})\ k$
⟨*proof*⟩

Chapter 2

Elementary properties of a valuation

2.1 Definition of a valuation

definition
valuation :: $[('b, 'm)$ *Ring-scheme*, $'b \Rightarrow$ *ant*$] \Rightarrow$ *bool* **where**
valuation $K\ v \longleftrightarrow$
$v \in$ *extensional* (*carrier* K) $\wedge$
$v \in$ *carrier* $K \to Z_\infty\ \wedge$
$v\ (\mathbf{0}_K) = \infty \wedge (\forall x{\in}((\text{carrier } K) - \{\mathbf{0}_K\}).\ v\ x \neq \infty) \wedge$
$(\forall x{\in}(\text{carrier } K).\ \forall y{\in}(\text{carrier } K).\ v\ (x \cdot_{r\,K} y) = (v\ x) + (v\ y)) \wedge$
$(\forall x{\in}(\text{carrier } K).\ 0 \leq (v\ x) \longrightarrow 0 \leq (v\ (1_{r\,K} \pm_K x))) \wedge$
$(\exists x.\ x \in \text{carrier } K \wedge (v\ x) \neq \infty \wedge (v\ x) \neq 0)$

lemma (**in** *Corps*) *invf-closed*:$x \in \text{carrier } K - \{\mathbf{0}\} \Longrightarrow x^{-\,K} \in \text{carrier } K$
⟨*proof*⟩

lemma (**in** *Corps*) *valuation-map*:*valuation* $K\ v \Longrightarrow v \in \text{carrier } K \to Z_\infty$
⟨*proof*⟩

lemma (**in** *Corps*) *value-in-aug-inf*:$[\![\text{valuation } K\ v;\ x \in \text{carrier } K]\!] \Longrightarrow$
$v\ x \in Z_\infty$
⟨*proof*⟩

lemma (**in** *Corps*) *value-of-zero*:*valuation* $K\ v \Longrightarrow v\ (\mathbf{0}) = \infty$
⟨*proof*⟩

lemma (**in** *Corps*) *val-nonzero-noninf*:$[\![\text{valuation } K\ v;\ x \in \text{carrier } K;\ x \neq \mathbf{0}]\!]$
$\Longrightarrow (v\ x) \neq \infty$
⟨*proof*⟩

lemma (**in** *Corps*) *value-inf-zero*:$[\![\text{valuation } K\ v;\ x \in \text{carrier } K;\ v\ x = \infty]\!]$
$\Longrightarrow x = \mathbf{0}$
⟨*proof*⟩

lemma (**in** *Corps*) *val-nonzero-z*:⟦*valuation K v*; *x* ∈ *carrier K*; *x* ≠ **0**⟧ ⟹
∃ *z*. (*v x*) = *ant z*
⟨*proof*⟩

lemma (**in** *Corps*) *val-nonzero-z-unique*:⟦*valuation K v*; *x* ∈ *carrier K*; *x* ≠ **0**⟧
⟹ ∃!*z*. (*v x*) = *ant z*
⟨*proof*⟩

lemma (**in** *Corps*) *value-noninf-nonzero*:⟦*valuation K v*; *x* ∈ *carrier K*; *v x* ≠ ∞⟧
⟹ *x* ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *val1-neq-0*:⟦*valuation K v*; *x* ∈ *carrier K*; *v x* = *1*⟧ ⟹
x ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *val-Zmin-sym*:⟦*valuation K v*; *x* ∈ *carrier K*; *y* ∈ *carrier K*⟧
⟹ *amin* (*v x*) (*v y*) = *amin* (*v y*) (*v x*)
⟨*proof*⟩

lemma (**in** *Corps*) *val-t2p*:⟦*valuation K v*; *x* ∈ *carrier K*; *y* ∈ *carrier K*⟧
⟹ *v* (*x* ·$_r$ *y*) = *v x* + *v y*
⟨*proof*⟩

lemma (**in** *Corps*) *val-axiom4*:⟦*valuation K v*; *x* ∈ *carrier K*; *0* ≤ *v x*⟧ ⟹
0 ≤ *v* (*1*$_r$ ± *x*)
⟨*proof*⟩

lemma (**in** *Corps*) *val-axiom5*:*valuation K v* ⟹
∃ *x*. *x* ∈ *carrier K* ∧ *v x* ≠ ∞ ∧ *v x* ≠ *0*
⟨*proof*⟩

lemma (**in** *Corps*) *val-field-nonzero*:*valuation K v* ⟹ *carrier K* ≠ {**0**}
⟨*proof*⟩

lemma (**in** *Corps*) *val-field-1-neq-0*:*valuation K v* ⟹ *1*$_r$ ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *value-of-one*:*valuation K v* ⟹ *v* (*1*$_r$) = *0*
⟨*proof*⟩

lemma (**in** *Corps*) *has-val-one-neq-zero*:*valuation K v* ⟹ *1*$_r$ ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *val-minus-one*:*valuation K v* ⟹ *v* (−$_a$ *1*$_r$) = *0*
⟨*proof*⟩

lemma (**in** *Corps*) *val-minus-eq*:⟦*valuation K v*; *x* ∈ *carrier K*⟧ ⟹

$$v\ (-_a\ x) = v\ x$$

⟨*proof*⟩

lemma (**in** *Corps*) *value-of-inv*:⟦*valuation K v*; $x \in$ *carrier K*; $x \neq \mathbf{0}$⟧ ⟹
$$v\ (x^{\text{-}K}) = -\ (v\ x)$$

⟨*proof*⟩

lemma (**in** *Corps*) *val-exp-ring*:⟦ *valuation K v*; $x \in$ *carrier K*; $x \neq \mathbf{0}$⟧
$$\Longrightarrow (int\ n) *_a\ (v\ x) = v\ (x^{\frown K\ n})$$

⟨*proof*⟩

exponent in a field

lemma (**in** *Corps*) *val-exp*:⟦ *valuation K v*; $x \in$ *carrier K*; $x \neq \mathbf{0}$⟧ ⟹
$$z *_a\ (v\ x) = v\ (x_K{}^z)$$

⟨*proof*⟩

lemma (**in** *Corps*) *value-zero-nonzero*:⟦*valuation K v*; $x \in$ *carrier K*; $v\ x = 0$⟧
$$\Longrightarrow x \neq \mathbf{0}$$

⟨*proof*⟩

lemma (**in** *Corps*) *v-ale-diff*:⟦*valuation K v*; $x \in$ *carrier K*; $y \in$ *carrier K*;
$x \neq \mathbf{0}$; $v\ x \leq v\ y$ ⟧ ⟹ $0 \leq v(y \cdot_r x^{\text{-}\ K})$

⟨*proof*⟩

lemma (**in** *Corps*) *amin-le-plusTr*:⟦*valuation K v*; $x \in$ *carrier K*; $y \in$ *carrier K*;
$v\ x \neq \infty$; $v\ y \neq \infty$; $v\ x \leq v\ y$⟧ ⟹ *amin* $(v\ x)\ (v\ y) \leq v\ (\ x \pm y)$

⟨*proof*⟩

lemma (**in** *Corps*) *amin-le-plus*:⟦*valuation K v*; $x \in$ *carrier K*; $y \in$ *carrier K*⟧
$$\Longrightarrow (amin\ (v\ x)\ (v\ y)) \leq (v\ (x \pm y))$$

⟨*proof*⟩

lemma (**in** *Corps*) *value-less-eq*:⟦ *valuation K v*; $x \in$ *carrier K*; $y \in$ *carrier K*;
$(v\ x) < (v\ y)$⟧ ⟹ $(v\ x) = (v\ (x \pm y))$

⟨*proof*⟩

lemma (**in** *Corps*) *value-less-eq1*:⟦*valuation K v*; $x \in$ *carrier K*; $y \in$ *carrier K*;
$(v\ x) < (v\ y)$⟧ ⟹ $v\ x = \ v\ (y \pm x)$

⟨*proof*⟩

lemma (**in** *Corps*) *val-1px*:⟦*valuation K v*; $x \in$ *carrier K*; $0 \leq (v\ (1_r \pm x))$⟧
$$\Longrightarrow 0 \leq (v\ x)$$

⟨*proof*⟩

lemma (**in** *Corps*) *val-1mx*:⟦*valuation K v*; $x \in$ *carrier K*;
$0 \leq (v\ (1_r \pm (-_a\ x)))$⟧ ⟹ $0 \leq (v\ x)$

⟨*proof*⟩

2.2 The normal valuation of v

definition
$Lv :: [('r, 'm)\ Ring\text{-}scheme\ , 'r \Rightarrow ant] \Rightarrow ant$ **where**
$Lv\ K\ v = AMin\ \{x.\ x \in v\ `\ carrier\ K \wedge 0 < x\}$

definition
$n\text{-}val :: [('r, 'm)\ Ring\text{-}scheme, 'r \Rightarrow ant] \Rightarrow ('r \Rightarrow ant)$ **where**
$n\text{-}val\ K\ v = (\lambda x{\in}\ carrier\ K.\ \ (THE\ l.\ (l * (Lv\ K\ v)) = v\ x))$

definition
$Pg :: [('r, 'm)\ Ring\text{-}scheme, 'r \Rightarrow ant] \Rightarrow 'r$ **where**
$Pg\ K\ v = (SOME\ x.\ x \in carrier\ K - \{\mathbf{0}_K\} \wedge v\ x = Lv\ K\ v)$

lemma (**in** *Corps*) *vals-pos-nonempty*:*valuation K v* $\Longrightarrow$
$\{x.\ x \in v\ `\ carrier\ K \wedge 0 < x\} \neq \{\}$
⟨*proof*⟩

lemma (**in** *Corps*) *vals-pos-LBset*:*valuation K v* $\Longrightarrow$
$\{x.\ x \in v\ `\ carrier\ K \wedge 0 < x\} \subseteq LBset\ 1$
⟨*proof*⟩

lemma (**in** *Corps*) *Lv-pos*:*valuation K v* $\Longrightarrow 0 < Lv\ K\ v$
⟨*proof*⟩

lemma (**in** *Corps*) *AMin-z*:*valuation K v* $\Longrightarrow$
$\exists\, a.\ AMin\ \{x.\ x \in v\ `\ carrier\ K \wedge 0 < x\} = ant\ a$
⟨*proof*⟩

lemma (**in** *Corps*) *Lv-z*:*valuation K v* $\Longrightarrow \exists\, z.\ Lv\ K\ v = ant\ z$
⟨*proof*⟩

lemma (**in** *Corps*) *AMin-k*:*valuation K v* $\Longrightarrow$
$\exists\, k{\in}\ carrier\ K - \{\mathbf{0}\}.\ AMin\ \{x.\ x \in v\ `\ carrier\ K \wedge 0 < x\} = v\ k$

⟨*proof*⟩

lemma (**in** *Corps*) *val-Pg*: *valuation K v* $\Longrightarrow$
$Pg\ K\ v \in carrier\ K - \{\mathbf{0}\} \wedge v\ (Pg\ K\ v) = Lv\ K\ v$
⟨*proof*⟩

lemma (**in** *Corps*) *amin-generateTr*:*valuation K v* $\Longrightarrow$
$\forall\, w{\in}carrier\ K - \{\mathbf{0}\}.\ \exists\, z.\ v\ w = z *_a\ AMin\ \{x.\ x \in v\ `\ carrier\ K \wedge 0 < x\}$
⟨*proof*⟩

lemma (**in** *Corps*) *val-principalTr1*:$[\![$ *valuation K v*$]\!]$ $\Longrightarrow$
$Lv\ K\ v \in v\ `\ (carrier\ K - \{\mathbf{0}\}) \wedge$
$(\forall\, w{\in}v\ `\ carrier\ K.\ \exists\, a.\ w = a * Lv\ K\ v) \wedge 0 < Lv\ K\ v$

⟨*proof*⟩

lemma (**in** *Corps*) *val-principalTr2*:⟦*valuation K v*;
$c \in v$ ‘ (*carrier K* − {**0**}) ∧ (∀ *w*∈*v* ‘ *carrier K*. ∃ *a*. *w* = *a* ∗ *c*) ∧ *0* < *c*;
$d \in v$ ‘ (*carrier K* − {**0**}) ∧ (∀ *w*∈*v* ‘ *carrier K*. ∃ *a*. *w* = *a* ∗ *d*) ∧ *0* < *d*⟧
⟹ *c* = *d*
⟨*proof*⟩

lemma (**in** *Corps*) *val-principal*:*valuation K v* ⟹
∃!*x0*. *x0* ∈ *v* ‘ (*carrier K* − {**0**}) ∧
(∀ *w* ∈ *v* ‘ (*carrier K*). ∃ (*a*::*ant*). *w* = *a* ∗ *x0*) ∧ *0* < *x0*
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-defTr*:⟦*valuation K v*; *w* ∈ *carrier K*⟧ ⟹
∃!*a*. *a* ∗ *Lv K v* = *v w*
⟨*proof*⟩

lemma (**in** *Corps*) *n-valTr*:⟦ *valuation K v*; *x* ∈ *carrier K*⟧ ⟹
(*THE l*. (*l* ∗ (*Lv K v*)) = *v x*)∗(*Lv K v*) = *v x*
⟨*proof*⟩

lemma (**in** *Corps*) *n-val*:⟦*valuation K v*; *x* ∈ *carrier K*⟧ ⟹
(*n-val K v x*)∗(*Lv K v*) = *v x*
⟨*proof*⟩

lemma (**in** *Corps*) *val-pos-n-val-pos*:⟦*valuation K v*; *x* ∈ *carrier K*⟧ ⟹
(*0* ≤ *v x*) = (*0* ≤ *n-val K v x*)
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-in-aug-inf*:⟦*valuation K v*; *x* ∈ *carrier K*⟧ ⟹
n-val K v x ∈ Z_∞
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-0*:⟦*valuation K v*; *x* ∈ *carrier K*; *v x* = *0*⟧
⟹ *n-val K v x* = *0*
⟨*proof*⟩

lemma (**in** *Corps*) *value-n0-n-val-n0*:⟦*valuation K v*; *x* ∈ *carrier K*; *v x* ≠ *0*⟧ ⟹
n-val K v x ≠ *0*
⟨*proof*⟩

lemma (**in** *Corps*) *val-0-n-val-0*:⟦*valuation K v*; *x* ∈ *carrier K*⟧ ⟹
(*v x* = *0*) = (*n-val K v x* = *0*)
⟨*proof*⟩

lemma (**in** *Corps*) *val-noninf-n-val-noninf*:⟦*valuation K v*; *x* ∈ *carrier K*⟧ ⟹
(*v x* ≠ ∞) = (*n-val K v x* ≠ ∞)
⟨*proof*⟩

lemma (**in** *Corps*) *val-inf-n-val-inf*:⟦*valuation K v*; $x \in$ *carrier K*⟧ ⟹
$(v\ x = \infty) = (n\text{-}val\ K\ v\ x = \infty)$
⟨*proof*⟩

lemma (**in** *Corps*) *val-eq-n-val-eq*:⟦*valuation K v*; $x \in$ *carrier K*; $y \in$ *carrier K*⟧
⟹ $(v\ x = v\ y) = (n\text{-}val\ K\ v\ x = n\text{-}val\ K\ v\ y)$
⟨*proof*⟩

lemma (**in** *Corps*) *val-poss-n-val-poss*:⟦*valuation K v*; $x \in$ *carrier K*⟧ ⟹
$(0 < v\ x) = (0 < n\text{-}val\ K\ v\ x)$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-Pg*:*valuation K v* ⟹ $n\text{-}val\ K\ v\ (Pg\ K\ v) = 1$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-valuationTr1*:*valuation K v* ⟹
$\forall x \in$ *carrier K*. $n\text{-}val\ K\ v\ x \in Z_\infty$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-t2p*:⟦*valuation K v*; $x \in$ *carrier K*; $y \in$ *carrier K*⟧ ⟹
$n\text{-}val\ K\ v\ (x \cdot_r y) = n\text{-}val\ K\ v\ x + (n\text{-}val\ K\ v\ y)$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-valuationTr2*:⟦ *valuation K v*; $x \in$ *carrier K*;
$y \in$ *carrier K*⟧ ⟹
$amin\ (n\text{-}val\ K\ v\ x)\ (n\text{-}val\ K\ v\ y) \leq (n\text{-}val\ K\ v\ (\ x \pm y))$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-valuation*:*valuation K v* ⟹
valuation K $(n\text{-}val\ K\ v)$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-le-val*:⟦*valuation K v*; $x \in$ *carrier K*; $0 \leq (v\ x)$⟧ ⟹
$(n\text{-}val\ K\ v\ x) \leq (v\ x)$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-surj*:*valuation K v* ⟹
$\exists x \in$ *carrier K*. $n\text{-}val\ K\ v\ x = 1$
⟨*proof*⟩

lemma (**in** *Corps*) *n-value-in-aug-inf*:⟦*valuation K v*; $x \in$ *carrier K*⟧ ⟹
$n\text{-}val\ K\ v\ x \in Z_\infty$
⟨*proof*⟩

lemma (**in** *Corps*) *val-surj-n-valTr*:⟦*valuation K v*; $\exists x \in$ *carrier K*. $v\ x = 1$⟧
⟹ $Lv\ K\ v = 1$
⟨*proof*⟩

lemma (**in** *Corps*) *val-surj-n-val*:⟦*valuation K v*; $\exists x \in$ *carrier K*. $v\ x = 1$⟧ ⟹

$(n\text{-}val\ K\ v) = v$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-n-val*:*valuation K v* ⟹
$n\text{-}val\ K\ (n\text{-}val\ K\ v) = n\text{-}val\ K\ v$
⟨*proof*⟩

lemma *nnonzero-annonzero*:$0 < N \Longrightarrow an\ N \neq 0$
⟨*proof*⟩

2.3 Valuation ring

definition
$Vr :: [('r, 'm)\ Ring\text{-}scheme, 'r \Rightarrow ant] \Rightarrow ('r, 'm)\ Ring\text{-}scheme$ **where**
$Vr\ K\ v = Sr\ K\ (\{x.\ x \in carrier\ K \wedge 0 \leq (v\ x)\})$

definition
$vp :: [('r, 'm)\ Ring\text{-}scheme, 'r \Rightarrow ant] \Rightarrow 'r\ set$ **where**
$vp\ K\ v = \{x.\ x \in carrier\ (Vr\ K\ v) \wedge 0 < (v\ x)\}$

definition
$r\text{-}apow :: [('r, 'm)\ Ring\text{-}scheme, 'r\ set, ant] \Rightarrow 'r\ set$ **where**
$r\text{-}apow\ R\ I\ a = (if\ a = \infty\ then\ \{\mathbf{0}_R\}\ else$
$(if\ a = 0\ then\ carrier\ R\ else\ I^{\diamondsuit R\ (na\ a)}))$

abbreviation
$RAPOW\ \ ((3\text{-}^{\ }\text{-}^{\ })\ [62,62,63]62)$ **where**
$I^{R\ a} == r\text{-}apow\ R\ I\ a$

lemma (**in** *Ring*) *ring-pow-apow*:*ideal R I* ⟹
$I^{\diamondsuit R\ n} = I^{R\ (an\ n)}$
⟨*proof*⟩

lemma (**in** *Ring*) *r-apow-Suc*:*ideal R I* ⟹ $I^{R\ (an\ (Suc\ 0))} = I$
⟨*proof*⟩

lemma (**in** *Ring*) *apow-ring-pow*:*ideal R I* ⟹
$I^{\diamondsuit R\ n} = I^{R\ (an\ n)}$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-ring*:*valuation K v* ⟹ *Ring* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *val-pos-mem-Vr*:⟦*valuation K v*; $x \in carrier\ K$⟧ ⟹
$(0 \leq (v\ x)) = (x \in carrier\ (Vr\ K\ v))$
⟨*proof*⟩

lemma (**in** *Corps*) *val-poss-mem-Vr*:⟦*valuation K v*; *x* ∈ *carrier K*; *0* < (*v x*)⟧
⟹ *x* ∈ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-one*:*valuation K v* ⟹ $1_{r\,K}$ ∈ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-mem-f-mem*:⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*)⟧
⟹ *x* ∈ *carrier K*
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-0-f-0*:*valuation K v* ⟹ $\mathbf{0}_{Vr\ K\ v} = \mathbf{0}$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-1-f-1*:*valuation K v* ⟹ $1_{r(Vr\ K\ v)} = 1_r$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-pOp-f-pOp*:⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*);
y ∈ *carrier* (*Vr K v*)⟧ ⟹ $x \pm_{Vr\ K\ v} y = x \pm y$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-mOp-f-mOp*:⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*)⟧
⟹ $-_{a(Vr\ K\ v)}\ x = -_a\ x$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-tOp-f-tOp*:⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*);
y ∈ *carrier*(*Vr K v*)⟧ ⟹ $x \cdot_{r(Vr\ K\ v)} y = x \cdot_r y$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-pOp-le*:⟦*valuation K v*; *x* ∈ *carrier K*;
y ∈ *carrier* (*Vr K v*)⟧ ⟹ *v x* ≤ (*v x* + (*v y*))
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-integral*:*valuation K v* ⟹ *Idomain* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-exp-mem*:⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*)⟧
⟹ $x^{\frown K\ n}$ ∈ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-exp-f-exp*:⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*)⟧ ⟹
$x^{\frown(Vr\ K\ v)\ n} = x^{\frown K\ n}$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-potent-nonzero*:⟦*valuation K v*;
x ∈ *carrier* (*Vr K v*) − {$\mathbf{0}_{Vr\ K\ v}$}⟧ ⟹ $x^{\frown K\ n} \neq \mathbf{0}_{Vr\ K\ v}$
⟨*proof*⟩

lemma (**in** *Corps*) *elem-0-val-if*:⟦*valuation K v*; *x* ∈ *carrier K*; *v x* = *0*⟧
⟹ *x* ∈ *carrier* (*Vr K v*) ∧ $x^{-\,K}$ ∈ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *elem0val*:⟦*valuation K v*; *x* ∈ *carrier K*; *x* ≠ **0**⟧ ⟹
(*v x* = *0*) = (*x* ∈ *carrier* (*Vr K v*) ∧ $x^{-\,K}$ ∈ *carrier* (*Vr K v*))
⟨*proof*⟩

lemma (**in** *Corps*) *ideal-inc-elem0val-whole*:⟦ *valuation K v*; *x* ∈ *carrier K*;
v x = *0*; *ideal* (*Vr K v*) *I*; *x* ∈ *I*⟧ ⟹ *I* = *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *vp-mem-Vr-mem*:⟦*valuation K v*; *x* ∈ (*vp K v*)⟧ ⟹
x ∈ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *vp-mem-val-poss*:⟦ *valuation K v*; *x* ∈ *carrier K*⟧ ⟹
(*x* ∈ *vp K v*) = (*0* < (*v x*))
⟨*proof*⟩

lemma (**in** *Corps*) *Pg-in-Vr*:*valuation K v* ⟹ *Pg K v* ∈ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *vp-ideal*:*valuation K v* ⟹ *ideal* (*Vr K v*) (*vp K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *vp-not-whole*:*valuation K v* ⟹
(*vp K v*) ≠ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Ring*) *elem-out-ideal-nonzero*:⟦*ideal R I*; *x* ∈ *carrier R*;
x ∉ *I*⟧ ⟹ *x* ≠ $\mathbf{0}_R$
⟨*proof*⟩

lemma (**in** *Corps*) *vp-prime*:*valuation K v* ⟹ *prime-ideal* (*Vr K v*) (*vp K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *vp-pow-ideal*:*valuation K v* ⟹
ideal (*Vr K v*) ($(vp\ K\ v)^{\Diamond(Vr\ K\ v)\ n}$)
⟨*proof*⟩

lemma (**in** *Corps*) *vp-apow-ideal*:⟦*valuation K v*; *0* ≤ *n*⟧ ⟹
ideal (*Vr K v*) ($(vp\ K\ v)^{(Vr\ K\ v)\ n}$)
⟨*proof*⟩

lemma (**in** *Corps*) *mem-vp-apow-mem-Vr*:⟦*valuation K v*;
0 ≤ *N*; *x* ∈ *vp K v* $^{(Vr\ K\ v)\ N}$⟧ ⟹ *x* ∈ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *elem-out-vp-unit*:⟦*valuation K v*; $x \in$ *carrier* (*Vr K v*); $x \notin$ *vp K v*⟧ $\Longrightarrow$ *v x* = *0*
⟨*proof*⟩

lemma (**in** *Corps*) *vp-maximal*:*valuation K v* $\Longrightarrow$ *maximal-ideal* (*Vr K v*) (*vp K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *ideal-sub-vp*:⟦ *valuation K v*; *ideal* (*Vr K v*) *I*; *I* ≠ *carrier* (*Vr K v*)⟧ $\Longrightarrow$ *I* ⊆ (*vp K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-local*:⟦*valuation K v*; *maximal-ideal* (*Vr K v*) *I*⟧ $\Longrightarrow$ (*vp K v*) = *I*
⟨*proof*⟩

lemma (**in** *Corps*) *v-residue-field*:*valuation K v* $\Longrightarrow$ *Corps* ((*Vr K v*) /$_r$ (*vp K v*))
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-n-val-Vr*:*valuation K v* $\Longrightarrow$ *carrier* (*Vr K v*) = *carrier* (*Vr K* (*n-val K v*))
⟨*proof*⟩

2.4 Ideals in a valuation ring

lemma (**in** *Corps*) *Vr-has-poss-elem*:*valuation K v* $\Longrightarrow$ ∃ *x*∈*carrier* (*Vr K v*) − {**0**$_{Vr\ K\ v}$}. *0* < *v x*
⟨*proof*⟩

lemma (**in** *Corps*) *vp-nonzero*:*valuation K v* $\Longrightarrow$ *vp K v* ≠ {**0**$_{Vr\ K\ v}$}
⟨*proof*⟩

lemma (**in** *Corps*) *field-frac-mul*:⟦*x* ∈ *carrier K*; *y* ∈ *carrier K*; *y* ≠ **0**⟧ $\Longrightarrow$ *x* = (*x* ·$_r$ (*y*$^{-K}$)) ·$_r$ *y*
⟨*proof*⟩

lemma (**in** *Corps*) *elems-le-val*:⟦*valuation K v*; *x* ∈ *carrier K*; *y* ∈ *carrier K*; *x* ≠ **0**; *v x* ≤ (*v y*)⟧ $\Longrightarrow$ ∃ *r*∈*carrier* (*Vr K v*). *y* = *r* ·$_r$ *x*
⟨*proof*⟩

lemma (**in** *Corps*) *val-Rxa-gt-a*:⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*) − {**0**}; *y* ∈ *carrier* (*Vr K v*); *y* ∈ *Rxa* (*Vr K v*) *x*⟧ $\Longrightarrow$ *v x* ≤ (*v y*)
⟨*proof*⟩

lemma (**in** *Corps*) *val-Rxa-gt-a-1*:⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*); *y* ∈ *carrier* (*Vr K v*); *x* ≠ **0**; *v x* ≤ (*v y*)⟧ $\Longrightarrow$ *y* ∈ *Rxa* (*Vr K v*) *x*
⟨*proof*⟩

lemma (**in** *Corps*) *eqval-inv*:⟦*valuation K v*; *x* ∈ *carrier K*; *y* ∈ *carrier K*;
y ≠ **0**; *v x* = *v y*⟧ ⟹ *0* = *v* (*x* ·$_r$ (*y*$^{-K}$))
⟨*proof*⟩

lemma (**in** *Corps*) *eq-val-eq-idealTr*:⟦*valuation K v*;
x ∈ *carrier* (*Vr K v*) − {**0**}; *y* ∈ *carrier* (*Vr K v*); *v x* ≤ (*v y*)⟧ ⟹
Rxa (*Vr K v*) *y* ⊆ *Rxa* (*Vr K v*) *x*
⟨*proof*⟩

lemma (**in** *Corps*) *eq-val-eq-ideal*:⟦*valuation K v*;
x ∈ *carrier* (*Vr K v*); *y* ∈ *carrier* (*Vr K v*); *v x* = *v y*⟧
⟹ *Rxa* (*Vr K v*) *x* = *Rxa* (*Vr K v*) *y*
⟨*proof*⟩

lemma (**in** *Corps*) *eq-ideal-eq-val*:⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*);
y ∈ *carrier* (*Vr K v*); *Rxa* (*Vr K v*) *x* = *Rxa* (*Vr K v*) *y*⟧ ⟹ *v x* = *v y*
⟨*proof*⟩

lemma (**in** *Corps*) *zero-val-gen-whole*:
⟦*valuation K v*; *x* ∈ *carrier* (*Vr K v*)⟧ ⟹
(*v x* = *0*) = (*Rxa* (*Vr K v*) *x* = *carrier* (*Vr K v*))
⟨*proof*⟩

lemma (**in** *Corps*) *elem-nonzeroval-gen-proper*:⟦ *valuation K v*;
x ∈ *carrier* (*Vr K v*); *v x* ≠ *0*⟧ ⟹ *Rxa* (*Vr K v*) *x* ≠ *carrier* (*Vr K v*)
⟨*proof*⟩

We prove that Vr K v is a principal ideal ring

definition
LI :: [('*r*, '*m*) *Ring-scheme*, '*r* ⇒ *ant*, '*r set*] ⇒ *ant* **where**

LI K v I = *AMin* (*v* ‘ *I*)

definition
Ig :: [('*r*, '*m*) *Ring-scheme*, '*r* ⇒ *ant*, '*r set*] ⇒ '*r* **where**

Ig K v I = (*SOME x*. *x* ∈ *I* ∧ *v x* = *LI K v I*)

lemma (**in** *Corps*) *val-in-image*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*; *x* ∈ *I*⟧ ⟹
v x ∈ *v* ‘ *I*
⟨*proof*⟩

lemma (**in** *Corps*) *I-vals-nonempty*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*⟧ ⟹
v ‘ *I* ≠ {}
⟨*proof*⟩

lemma (**in** *Corps*) *I-vals-LBset*:⟦ *valuation K v*; *ideal* (*Vr K v*) *I*⟧ ⟹
v ‘ *I* ⊆ *LBset 0*
⟨*proof*⟩

lemma (**in** *Corps*) *LI-pos*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*⟧ ⟹ *0* ≤ *LI K v I*
⟨*proof*⟩

lemma (**in** *Corps*) *LI-poss*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*;
I ≠ *carrier* (*Vr K v*)⟧ ⟹ *0* < *LI K v I*
⟨*proof*⟩

lemma (**in** *Corps*) *LI-z*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*; *I* ≠ {**0**$_{Vr\ K\ v}$}⟧ ⟹
∃ *z*. *LI K v I* = *ant z*
⟨*proof*⟩

lemma (**in** *Corps*) *LI-k*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*⟧ ⟹
∃ *k*∈ *I*. *LI K v I* = *v k*
⟨*proof*⟩

lemma (**in** *Corps*) *LI-infinity*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*⟧ ⟹
(*LI K v I* = ∞) = (*I* = {**0**$_{Vr\ K\ v}$})
⟨*proof*⟩

lemma (**in** *Corps*) *val-Ig*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*⟧ ⟹
(*Ig K v I*) ∈ *I* ∧ *v* (*Ig K v I*) = *LI K v I*
⟨*proof*⟩

lemma (**in** *Corps*) *Ig-nonzero*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*; *I* ≠ {**0**$_{Vr\ K\ v}$}⟧
⟹ (*Ig K v I*) ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-ideal-npowf-closed*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*;
x ∈ *I*; *0* < *n*⟧ ⟹ $x_K{}^n$ ∈ *I*
⟨*proof*⟩

lemma (**in** *Corps*) *Ig-generate-I*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*⟧ ⟹
(*Vr K v*) ◇$_p$ (*Ig K v I*) = *I*
⟨*proof*⟩

lemma (**in** *Corps*) *Pg-gen-vp*:*valuation K v* ⟹
(*Vr K v*) ◇$_p$ (*Pg K v*) = *vp K v*
⟨*proof*⟩

lemma (**in** *Corps*) *vp-gen-t*:*valuation K v* ⟹
∃ *t*∈*carrier* (*Vr K v*). *vp K v* = (*Vr K v*) ◇$_p$ *t*
⟨*proof*⟩

lemma (**in** *Corps*) *vp-gen-nonzero*:⟦*valuation K v*; *vp K v* = (*Vr K v*) ◇$_p$ *t*⟧ ⟹
t ≠ **0**$_{Vr\ K\ v}$
⟨*proof*⟩

lemma (**in** *Corps*) *n-value-idealTr*:⟦*valuation K v*; *0* ≤ *n*⟧ ⟹

$(vp\ K\ v)\ ^{\diamondsuit(Vr\ K\ v)\ n} = Vr\ K\ v\ \diamondsuit_p\ ((Pg\ K\ v)^{\frown(Vr\ K\ v)\ n})$
⟨*proof*⟩

lemma (**in** *Corps*) *ideal-pow-vp*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*;
$I \neq carrier\ (Vr\ K\ v)$; $I \neq \{\mathbf{0}_{Vr\ K\ v}\}$⟧ ⟹
$I = (vp\ K\ v)^{\diamondsuit}\ (Vr\ K\ v)\ (na\ (n\text{-}val\ K\ v\ (Ig\ K\ v\ I)))$
⟨*proof*⟩

lemma (**in** *Corps*) *ideal-apow-vp*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*⟧ ⟹
$I = (vp\ K\ v)\ (Vr\ K\ v)\ (n\text{-}val\ K\ v\ (Ig\ K\ v\ I))$
⟨*proof*⟩

lemma (**in** *Corps*) *ideal-apow-n-val*:⟦*valuation K v*; $x \in carrier\ (Vr\ K\ v)$⟧ ⟹
$(Vr\ K\ v)\ \diamondsuit_p\ x = (vp\ K\ v)^{(Vr\ K\ v)\ (n\text{-}val\ K\ v\ x)}$
⟨*proof*⟩

lemma (**in** *Corps*) *t-gen-vp*:⟦*valuation K v*; $t \in carrier\ K$; $v\ t = 1$⟧ ⟹
$(Vr\ K\ v)\ \diamondsuit_p\ t = vp\ K\ v$

⟨*proof*⟩

lemma (**in** *Corps*) *t-vp-apow*:⟦*valuation K v*; $t \in carrier\ K$; $v\ t = 1$⟧ ⟹
$(Vr\ K\ v)\ \diamondsuit_p\ (t^{\frown(Vr\ K\ v)\ n}) = (vp\ K\ v)^{(Vr\ K\ v)\ (an\ n)}$

⟨*proof*⟩

lemma (**in** *Corps*) *nonzeroelem-gen-nonzero*:⟦*valuation K v*; $x \neq \mathbf{0}$;
$x \in carrier\ (Vr\ K\ v)$⟧ ⟹ $Vr\ K\ v\ \diamondsuit_p\ x \neq \{\mathbf{0}_{Vr\ K\ v}\}$
⟨*proof*⟩

2.4.1 Amin lemma (in Corps)s

lemma (**in** *Corps*) *Amin-le-addTr*:*valuation K v* ⟹
$(\forall j \leq n.\ f\ j \in carrier\ K) \longrightarrow Amin\ n\ (v \circ f) \leq (v\ (nsum\ K\ f\ n))$
⟨*proof*⟩

lemma (**in** *Corps*) *Amin-le-add*:⟦*valuation K v*; $\forall j \leq n.\ f\ j \in carrier\ K$⟧ ⟹
$Amin\ n\ (v \circ f) \leq (v\ (nsum\ K\ f\ n))$
⟨*proof*⟩

lemma (**in** *Corps*) *value-ge-add*:⟦*valuation K v*; $\forall j \leq n.\ f\ j \in carrier\ K$;
$\forall j \leq n.\ z \leq ((v \circ f)\ j)$⟧ ⟹ $z \leq (v\ (\Sigma_e\ K\ f\ n))$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-ideal-powTr1*:⟦*valuation K v*; *ideal* (*Vr K v*) *I*;

$I \neq carrier\ (Vr\ K\ v);\ b \in I\rrbracket \Longrightarrow b \in (vp\ K\ v)$
⟨*proof*⟩

2.5 pow of vp and *n-value* − convergence −

lemma (**in** *Corps*) *n-value-x-1*:⟦*valuation K v*; $0 \leq n$;
$x \in (vp\ K\ v)\ ^{(Vr\ K\ v)}\ n\rrbracket \Longrightarrow\ n \leq (n\text{-}val\ K\ v\ x)$

⟨*proof*⟩

lemma (**in** *Corps*) *n-value-x-1-nat*:⟦*valuation K v*; $x \in (vp\ K\ v)^{\diamondsuit(Vr\ K\ v)\ n}\ \rrbracket \Longrightarrow$
$(an\ n) \leq (n\text{-}val\ K\ v\ x)$
⟨*proof*⟩

lemma (**in** *Corps*) *n-value-x-2*:⟦*valuation K v*; $x \in carrier\ (Vr\ K\ v)$;
$n \leq (n\text{-}val\ K\ v\ x);\ \ 0 \leq n\rrbracket \Longrightarrow\ x \in (vp\ K\ v)\ ^{(Vr\ K\ v)}\ n$
⟨*proof*⟩

lemma (**in** *Corps*) *n-value-x-2-nat*:⟦*valuation K v*; $x \in carrier\ (Vr\ K\ v)$;
$(an\ n) \leq ((n\text{-}val\ K\ v)\ x)\rrbracket \Longrightarrow\ x \in (vp\ K\ v)^{\diamondsuit(Vr\ K\ \ v)\ \ n}$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-n-pow*:⟦*valuation K v*; $x \in carrier\ (Vr\ K\ v)$; $0 \leq n\rrbracket \Longrightarrow$
$(n \leq (n\text{-}val\ K\ v\ x)) = (x \in (vp\ K\ v)\ ^{(Vr\ K\ v)}\ \ n)$
⟨*proof*⟩

lemma (**in** *Corps*) *eqval-in-vpr-apow*:⟦*valuation K v*; $x \in carrier\ K$; $0 \leq n$;
$y \in carrier\ K$; $n\text{-}val\ K\ v\ x = n\text{-}val\ K\ v\ y$; $x \in (vp\ K\ v)^{(Vr\ K\ v)\ n}\rrbracket \Longrightarrow$
$y \in (vp\ K\ v)\ ^{(Vr\ K\ v)\ n}$
⟨*proof*⟩

lemma (**in** *Corps*) *convergenceTr*:⟦*valuation K v*; $x \in carrier\ K$; $b \in carrier\ K$;
$b \in (vp\ K\ v)^{(Vr\ K\ v)\ n}$; $(Abs\ (n\text{-}val\ K\ v\ x)) \leq n\rrbracket \Longrightarrow$
$x \cdot_r b \in (vp\ K\ v)^{(Vr\ K\ v)\ (n\ +\ (n\text{-}val\ K\ v\ x))}$

⟨*proof*⟩

lemma (**in** *Corps*) *convergenceTr1*:⟦*valuation K v*; $x \in carrier\ K$;
$b \in (vp\ K\ v)^{(Vr\ K\ v)\ (n\ +\ Abs\ (n\text{-}val\ K\ v\ x))}$; $0 \leq n\rrbracket \Longrightarrow$
$x \cdot_r b \in (vp\ K\ v)\ ^{(Vr\ K\ v)\ n}$
⟨*proof*⟩

lemma (**in** *Corps*) *vp-potent-zero*:⟦*valuation K v*; $0 \leq n\rrbracket \Longrightarrow$
$(n = \infty) = (vp\ K\ v\ ^{(Vr\ K\ v)\ n} = \{\mathbf{0}_{Vr\ K\ v}\})$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-potent-eqTr1*:⟦*valuation K v*; *0* ≤ *n*; *0* ≤ *m*;
(vp K v) (Vr K v) n = (vp K v) (Vr K v) m; *m = 0*⟧ ⟹ *n = m*

⟨*proof*⟩

lemma (**in** *Corps*) *Vr-potent-eqTr2*:⟦*valuation K v*;
(vp K v) ◇(Vr K v) n = (vp K v) ◇(Vr K v) m⟧ ⟹ *n = m*

⟨*proof*⟩

lemma (**in** *Corps*) *Vr-potent-eq*:⟦*valuation K v*; *0* ≤ *n*; *0* ≤ *m*;
(vp K v) (Vr K v) n = (vp K v) (Vr K v) m⟧ ⟹ *n = m*
⟨*proof*⟩

the following two lemma (in Corps) s are used in completion of K

lemma (**in** *Corps*) *Vr-prime-maximalTr1*:⟦*valuation K v*; *x* ∈ *carrier (Vr K v)*;
Suc 0 < n⟧ ⟹ *x* ·$_{r(Vr\ K\ v)}$ *(x^K (n − Suc 0))* ∈ *(Vr K v) ◇$_p$ (x^K n)*
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-prime-maximalTr2*:⟦ *valuation K v*; *x* ∈ *vp K v*; *x* ≠ **0**;
Suc 0 < n⟧ ⟹ *x* ∉ *Vr K v ◇$_p$ (x^K n) ∧ x^K (n − Suc 0)* ∉ *(Vr K v) ◇$_p$*
(x^K n)
⟨*proof*⟩

lemma (**in** *Corps*) *Vring-prime-maximal*:⟦*valuation K v*; *prime-ideal (Vr K v) I*;
I ≠ {**0**$_{Vr\ K\ v}$}⟧ ⟹ *maximal-ideal (Vr K v) I*
⟨*proof*⟩

From the above lemma (in Corps) , we see that a valuation ring is of dimension one.

lemma (**in** *Corps*) *field-frac1*:⟦*1*$_r$ ≠ **0**; *x* ∈ *carrier K*⟧ ⟹ *x = x* ·$_r$ *((1*$_r$*)^-K)*
⟨*proof*⟩

lemma (**in** *Corps*) *field-frac2*:⟦*x* ∈ *carrier K*; *x* ≠ **0**⟧ ⟹ *x = (1*$_r$*)* ·$_r$ *((x^-K)^-K)*
⟨*proof*⟩

lemma (**in** *Corps*) *val-nonpos-inv-pos*:⟦*valuation K v*; *x* ∈ *carrier K*;
¬ *0* ≤ *(v x)*⟧ ⟹ *0 < (v (x^-K))*
⟨*proof*⟩

lemma (**in** *Corps*) *frac-Vr-is-K*:⟦*valuation K v*; *x* ∈ *carrier K*⟧ ⟹
∃ *s*∈*carrier (Vr K v)*. ∃ *t*∈*carrier (Vr K v) − {**0**}*. *x = s* ·$_r$ *(t^-K)*
⟨*proof*⟩

lemma (**in** *Corps*) *valuations-eqTr1*:⟦*valuation K v*; *valuation K v′*;

$Vr\ K\ v = Vr\ K\ v'; \forall x{\in}carrier\ (Vr\ K\ v).\ v\ x = v'\ x\rrbracket \Longrightarrow v = v'$
⟨*proof*⟩

lemma (**in** *Corps*) *ridmap-rhom*:⟦ *valuation K v*; *valuation K v'*;
carrier (*Vr K v*) ⊆ *carrier* (*Vr K v'*)⟧ ⟹
ridmap (*Vr K v*) ∈ *rHom* (*Vr K v*) (*Vr K v'*)
⟨*proof*⟩

lemma (**in** *Corps*) *contract-ideal*:⟦*valuation K v*; *valuation K v'*;
carrier (*Vr K v*) ⊆ *carrier* (*Vr K v'*)⟧ ⟹
ideal (*Vr K v*) (*carrier* (*Vr K v*) ∩ *vp K v'*)
⟨*proof*⟩

lemma (**in** *Corps*) *contract-prime*:⟦*valuation K v*; *valuation K v'*;
carrier (*Vr K v*) ⊆ *carrier* (*Vr K v'*)⟧ ⟹
prime-ideal (*Vr K v*) (*carrier* (*Vr K v*) ∩ *vp K v'*)
⟨*proof*⟩

lemma (**in** *Corps*) *valuation-equivTr*:⟦*valuation K v*; *valuation K v'*;
x ∈ *carrier K*; 0 < (*v' x*); *carrier* (*Vr K v*) ⊆ *carrier* (*Vr K v'*)⟧
⟹ 0 ≤ (*v x*)
⟨*proof*⟩

lemma (**in** *Corps*) *contract-maximal*:⟦*valuation K v*; *valuation K v'*;
carrier (*Vr K v*) ⊆ *carrier* (*Vr K v'*)⟧ ⟹
maximal-ideal (*Vr K v*) (*carrier* (*Vr K v*) ∩ *vp K v'*)
⟨*proof*⟩

2.6 Equivalent valuations

definition
v-equiv :: [- , *'r* ⇒ *ant*, *'r* ⇒ *ant*] ⇒ *bool* **where**
v-equiv K v1 v2 ⟷ *n-val K v1* = *n-val K v2*

lemma (**in** *Corps*) *valuation-equivTr1*:⟦*valuation K v*; *valuation K v'*;
∀ *x*∈*carrier K*. 0 ≤ (*v x*) ⟶ 0 ≤ (*v' x*)⟧ ⟹
carrier (*Vr K v*) ⊆ *carrier* (*Vr K v'*)
⟨*proof*⟩

lemma (**in** *Corps*) *valuation-equivTr2*:⟦*valuation K v*; *valuation K v'*;
carrier (*Vr K v*) ⊆ *carrier* (*Vr K v'*); *vp K v* = *carrier* (*Vr K v*) ∩ *vp K v'*⟧
⟹ *carrier* (*Vr K v'*) ⊆ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *eq-carr-eq-Vring*: ⟦*valuation K v*; *valuation K v'*;
carrier (*Vr K v*) = *carrier* (*Vr K v'*)⟧ ⟹ *Vr K v* = *Vr K v'*
⟨*proof*⟩

lemma (**in** *Corps*) *valuations-equiv*:⟦*valuation K v*; *valuation K v'*;
$\forall x \in$*carrier K*. $0 \leq (v\ x) \longrightarrow 0 \leq (v'\ x)$⟧ $\Longrightarrow$ *v-equiv K v v'*

⟨*proof*⟩

lemma (**in** *Corps*) *val-equiv-axiom1*:*valuation K v* $\Longrightarrow$ *v-equiv K v v*
⟨*proof*⟩

lemma (**in** *Corps*) *val-equiv-axiom2*:⟦ *valuation K v*; *valuation K v'*;
v-equiv K v v'⟧ $\Longrightarrow$ *v-equiv K v' v*
⟨*proof*⟩

lemma (**in** *Corps*) *val-equiv-axiom3*:⟦ *valuation K v*; *valuation K v'*;
valuation K v'; *v-equiv K v v'*; *v-equiv K v' v''*⟧ $\Longrightarrow$ *v-equiv K v v''*
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-equiv-val*:⟦ *valuation K v*⟧ $\Longrightarrow$
v-equiv K v (*n-val K v*)
⟨*proof*⟩

2.7 Prime divisors

definition
prime-divisor :: [-, *'b* $\Rightarrow$ *ant*] $\Rightarrow$
(*'b* $\Rightarrow$ *ant*) *set* ((*2P* _ _) [*96*,*97*]*96*) **where**
$P_{K\ v} = \{v'.$ *valuation K v'* $\wedge$ *v-equiv K v v'*$\}$

definition
prime-divisors :: - $\Rightarrow$ (*'b* $\Rightarrow$ *ant*) *set set* (*Pds*$_1$ *96*) **where**
$Pds_K = \{P. \exists v.$ *valuation K v* $\wedge$ $P = P_{K\ v}\ \}$

definition
normal-valuation-belonging-to-prime-divisor ::
[- , (*'b* $\Rightarrow$ *ant*) *set*] $\Rightarrow$ (*'b* $\Rightarrow$ *ant*) ((*ν*_ _) [*96*,*97*]*96*) **where**
$\nu_{K\ P} =$ *n-val K* (*SOME v*. $v \in P$)

lemma (**in** *Corps*) *val-in-P-valuation*:⟦*valuation K v*; $v' \in P_{K\ v}$⟧ $\Longrightarrow$
valuation K v'
⟨*proof*⟩

lemma (**in** *Corps*) *vals-in-P-equiv*:⟦ *valuation K v*; $v' \in P_{K\ v}$⟧ $\Longrightarrow$
v-equiv K v v'
⟨*proof*⟩

lemma (**in** *Corps*) *v-in-prime-v*:*valuation K v* $\Longrightarrow$ $v \in P_{K\ v}$
⟨*proof*⟩

lemma (**in** *Corps*) *some-in-prime-divisor*:*valuation K v* $\Longrightarrow$

$(SOME\ w.\ w \in P_{K\ v}) \in\ P_{K\ v}$
⟨*proof*⟩

lemma (**in** *Corps*) *valuation-some-in-prime-divisor*:*valuation K v*
$\Longrightarrow$ *valuation K* $(SOME\ w.\ w \in P_{K\ v})$
⟨*proof*⟩

lemma (**in** *Corps*) *valuation-some-in-prime-divisor1*:$P \in Pds \Longrightarrow$
valuation K $(SOME\ w.\ w \in P)$
⟨*proof*⟩

lemma (**in** *Corps*) *representative-of-pd-valuation*:
$P \in Pds \Longrightarrow$ *valuation K* $(\nu_{K\ P})$
⟨*proof*⟩

lemma (**in** *Corps*) *some-in-P-equiv*:*valuation K v* $\Longrightarrow$
v-equiv K v $(SOME\ w.\ w \in P_{K\ v})$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-n-val1*:$P \in Pds \Longrightarrow$ *n-val K* $(\nu_{K\ P}) = (\nu_{K\ P})$
⟨*proof*⟩

lemma (**in** *Corps*) *P-eq-val-equiv*:$[\![$*valuation K v*; *valuation K v'*$]\!] \Longrightarrow$
$(v\text{-}equiv\ K\ v\ v') = (P_{K\ v} =\ P_{K\ v'})$
⟨*proof*⟩

lemma (**in** *Corps*) *unique-n-valuation*:$[\![\ P \in Pds_K;\ P' \in Pds]\!] \Longrightarrow$
$(P = P') =\ (\nu_{K\ P} = \nu_{K\ P'})$
⟨*proof*⟩

lemma (**in** *Corps*) *n-val-representative*:$P \in Pds \Longrightarrow\ (\nu_{K\ P}) \in P$
⟨*proof*⟩

lemma (**in** *Corps*) *val-equiv-eq-pdiv*:$[\![\ P \in Pds_K;\ P' \in Pds_K;$ *valuation K v*;
valuation K v'; *v-equiv K v v'*; $v \in P;\ v' \in P'\ ]\!] \Longrightarrow\ P = P'$
⟨*proof*⟩

lemma (**in** *Corps*) *distinct-p-divisors*:$[\![\ P \in Pds_K;\ P' \in Pds_K]\!] \Longrightarrow$
$(\neg\ P = P') =\ (\neg$ *v-equiv K* $(\nu_{K\ P})\ (\nu_{K\ P'}))$
⟨*proof*⟩

2.8 Approximation

definition
valuations :: [- , *nat*, *nat* ⇒ ('*r* ⇒ *ant*)] ⇒ *bool* **where**
valuations K n vv ⟷ $(\forall j \leq n.$ *valuation K* $(vv\ j))$

definition
vals-nonequiv :: [-, *nat*, *nat* ⇒ ('*r* ⇒ *ant*)] ⇒ *bool* **where**

vals-nonequiv K n vv $\longleftrightarrow$ *valuations K n vv* $\wedge$
$(\forall j{\leq}n.\ \forall l \leq n.\ j \neq l \longrightarrow \neg$ (*v-equiv K* (*vv j*) (*vv l*)))

definition
Ostrowski-elem :: [-, *nat*, *nat* $\Rightarrow$ ('*b* $\Rightarrow$ *ant*), '*b*] $\Rightarrow$ *bool* **where**
Ostrowski-elem K n vv x $\longleftrightarrow$
$(0 <$ (*vv 0* ($1_r K \pm_K (-_a K$ *x*)))) $\wedge$ $(\forall j{\in}$*nset* (*Suc 0*) *n*. *0* $<$ (*vv j x*))

lemma (**in** *Corps*) *Ostrowski-elem-0*:⟦*vals-nonequiv K n vv*; *x* $\in$ *carrier K*;
Ostrowski-elem K n vv x⟧ $\Longrightarrow$ *0* $<$ (*vv 0* ($1_r \pm (-_a$ *x*)))
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-elem-Suc*:⟦*vals-nonequiv K n vv*; *x* $\in$ *carrier K*;
Ostrowski-elem K n vv x; *j* $\in$ *nset* (*Suc 0*) *n*⟧ $\Longrightarrow$ *0* $<$ (*vv j x*)
⟨*proof*⟩

lemma (**in** *Corps*) *vals-nonequiv-valuation*:⟦*vals-nonequiv K n vv*; *m* $\leq$ *n*⟧ $\Longrightarrow$
valuation K (*vv m*)
⟨*proof*⟩

lemma (**in** *Corps*) *vals-nonequiv*:⟦ *vals-nonequiv K* (*Suc* (*Suc n*)) *vv*;
i $\leq$ (*Suc* (*Suc n*)); *j* $\leq$ (*Suc* (*Suc n*)); *i* $\neq$ *j*⟧ $\Longrightarrow$
$\neg$ (*v-equiv K* (*vv i*) (*vv j*))
⟨*proof*⟩

lemma (**in** *Corps*) *skip-vals-nonequiv*:*vals-nonequiv K* (*Suc* (*Suc n*)) *vv* $\Longrightarrow$
vals-nonequiv K (*Suc n*) (*compose* {*l*. *l* $\leq$ (*Suc n*)} *vv* (*skip j*))
⟨*proof*⟩

lemma (**in** *Corps*) *not-v-equiv-reflex*:⟦*valuation K v*; *valuation K v'*;
$\neg$ *v-equiv K v v'*⟧ $\Longrightarrow$ $\neg$ *v-equiv K v' v*
⟨*proof*⟩

lemma (**in** *Corps*) *nonequiv-ex-Ostrowski-elem*:⟦*valuation K v*; *valuation K v'*;
$\neg$ *v-equiv K v v'*⟧ $\Longrightarrow$ $\exists x{\in}$*carrier K*. *0* $\leq$ (*v x*) $\wedge$ (*v' x*) $<$ *0*
⟨*proof*⟩

lemma (**in** *Corps*) *field-op-minus*:⟦*a* $\in$ *carrier K*; *b* $\in$ *carrier K*; *b* $\neq$ **0**⟧ $\Longrightarrow$
$-_a$ (*a* $\cdot_r$ (b^{-K})) = ($-_a$ *a*) $\cdot_r$ (b^{-K})
⟨*proof*⟩

lemma (**in** *Corps*) *field-one-plus-frac1*:⟦*a* $\in$ *carrier K*; *b* $\in$ *carrier K*; *b* $\neq$ **0**⟧
$\Longrightarrow$ $1_r \pm$ (*a* $\cdot_r$ (b^{-K})) = (*b* $\pm$ *a*) $\cdot_r$ (b^{-K})
⟨*proof*⟩

lemma (**in** *Corps*) *field-one-plus-frac2*:⟦*a* $\in$ *carrier K*; *b* $\in$ *carrier K*;
a $\pm$ *b* $\neq$ **0**⟧ $\Longrightarrow$ $1_r \pm (-_a$ (*a* $\cdot_r$ (*a* $\pm$ *b*)$^{-K}$)) = *b* $\cdot_r$ ((*a* $\pm$ *b*)$^{-K}$)

⟨*proof*⟩

lemma (**in** *Corps*) *field-one-plus-frac3*:⟦$x \in$ *carrier* K; $x \neq 1_r$;
$1_r \pm x \cdot_r (1_r \pm -_a\ x) \neq \mathbf{0}$ ⟧ ⟹
$1_r \pm -_a\ x \cdot_r (1_r \pm x \cdot_r (1_r \pm -_a\ x))^{-}{}^{K} =$
$(1_r \pm -_a\ x^{\frown K}\ (Suc\ (Suc\ 0))) \cdot_r (1_r \pm x \cdot_r (1_r \pm -_a\ x))^{-}{}^{K}$
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr1*:⟦ *valuation* K v; $s \in$ *carrier* K; $t \in$ *carrier* K;
$0 \leq (v\ s)$; $v\ t < 0$⟧ ⟹ $s \pm t \neq \mathbf{0}$
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr2*:⟦*valuation* K v; $s \in$ *carrier* K; $t \in$ *carrier* K;
$0 \leq (v\ s)$; $v\ t < 0$⟧ ⟹ $0 < (v\ (1_r \pm (-_a\ ((t \cdot_r ((s \pm t)^{-K}))))))$
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr3*:⟦*valuation* K v; $s \in$ *carrier* K; $t \in$ *carrier* K;
$0 \leq (v\ t)$; $v\ s < 0$⟧ ⟹ $0 < (v\ (t \cdot_r ((\ s \pm t)^{-K})))$
⟨*proof*⟩

lemma (**in** *Corps*) *restrict-Ostrowski-elem*:⟦ $x \in$ *carrier* K;
Ostrowski-elem K (*Suc* (*Suc* n)) vv x⟧ ⟹ *Ostrowski-elem* K (*Suc* n) vv x
⟨*proof*⟩

lemma (**in** *Corps*) *restrict-vals-nonequiv*:*vals-nonequiv* K (*Suc* (*Suc* n)) vv ⟹
vals-nonequiv K (*Suc* n) vv
⟨*proof*⟩

lemma (**in** *Corps*) *restrict-vals-nonequiv1*:*vals-nonequiv* K (*Suc* (*Suc* n)) vv ⟹
vals-nonequiv K (*Suc* n) (*compose* {h. $h \leq$ (*Suc* n)} vv (*skip* 1))
⟨*proof*⟩

lemma (**in** *Corps*) *restrict-vals-nonequiv2*:⟦*vals-nonequiv* K (*Suc* (*Suc* n)) vv⟧
⟹ *vals-nonequiv* K (*Suc* n) (*compose* {j. $j \leq$ (*Suc* n)} vv (*skip* 2))
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr31*:⟦*valuation* K v; $s \in$ *carrier* K;
$0 < (v\ (1_r \pm (-_a\ s)))$⟧ ⟹ $s \neq \mathbf{0}$
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr32*:⟦*valuation* K v; $s \in$ *carrier* K;
$0 < (v\ (1_r \pm (-_a\ s)))$⟧ ⟹ $0 \leq (v\ s)$
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr4*:⟦*valuation* K v; $s \in$ *carrier* K; $t \in$ *carrier* K;
$0 < (v\ (1_r \pm (-_a\ s)))$; $0 < (v\ (1_r \pm (-_a\ t)))$⟧ ⟹
$0 < (v\ (1_r \pm (-_a\ (s \cdot_r t))))$
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr5*:⟦ *vals-nonequiv K* (*Suc* (*Suc n*)) *vv*;
s ∈ *carrier K*; *t* ∈ *carrier K*;
0 ≤ (*vv* (*Suc 0*)) *s* ∧ *0* ≤ (*vv* (*Suc* (*Suc 0*))) *t*;
Ostrowski-elem K (*Suc n*) (*compose* {*j*. *j* ≤ (*Suc n*)} *vv* (*skip 1*)) *s*;
Ostrowski-elem K (*Suc n*) (*compose* {*j*. *j* ≤ (*Suc n*)} *vv* (*skip 2*)) *t*⟧ ⟹
Ostrowski-elem K (*Suc* (*Suc n*)) *vv* (*s* ·$_r$ *t*)
⟨*proof*⟩

lemma (**in** *Corps*) *one-plus-x-nonzero*:⟦*valuation K v*; *x* ∈ *carrier K*; *v x* < *0*⟧
⟹ *1*$_r$ ± *x* ∈ *carrier K* ∧ *v* (*1*$_r$ ± *x*) < *0*
⟨*proof*⟩

lemma (**in** *Corps*) *val-neg-nonzero*:⟦*valuation K v*; *x* ∈ *carrier K*; *v x* < *0*⟧ ⟹
x ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr6*:⟦*valuation K v*; *x* ∈ *carrier K*; ¬ *0* ≤ (*v x*)⟧ ⟹
(*1*$_r$ ± *x* ·$_r$ (*1*$_r$ ± −$_a$ *x*)) ∈ *carrier K* − {**0**}
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr7*:⟦*valuation K v*; *x* ∈ *carrier K*; ¬ *0* ≤ (*v x*)⟧ ⟹
1$_r$ ± −$_a$ (*x* ·$_r$ ((*1*$_r$ ± *x* ·$_r$ (*1*$_r$ ± −$_a$ *x*))$^{-K}$)) =
(*1*$_r$ ± −$_a$ *x* ± *x* ·$_r$ (*1*$_r$ ± −$_a$ *x*)) ·$_r$ ((*1*$_r$ ± *x* ·$_r$ (*1*$_r$ ± −$_a$ *x*))$^{-K}$)
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-elem-nonzero*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
x ∈ *carrier K*; *Ostrowski-elem K* (*Suc n*) *vv x*⟧ ⟹ *x* ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-elem-not-one*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
x ∈ *carrier K*; *Ostrowski-elem K* (*Suc n*) *vv x*⟧ ⟹ *1*$_r$ ± −$_a$ *x* ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *val-unit-cond*:⟦ *valuation K v*; *x* ∈ *carrier K*;
0 < (*v* (*1*$_r$ ± −$_a$ *x*))⟧ ⟹ *v x* = *0*
⟨*proof*⟩

end

theory *Valuation2*
imports *Valuation1*
begin

lemma (**in** *Corps*) *OstrowskiTr8*:⟦*valuation K v*; *x* ∈ *carrier K*;
0 < *v* (*1*$_r$ ± −$_a$ *x*)⟧ ⟹
0 < (*v* (*1*$_r$ ± −$_a$ (*x* ·$_r$ ((*1*$_r$ ± *x* ·$_r$ (*1*$_r$ ± −$_a$ *x*))$^{-K}$))))
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr9*:⟦*valuation K v*; *x* ∈ *carrier K*; *0* < (*v x*)⟧ ⟹
0 < (*v* (*x* ·$_r$ ((*1*$_r$ ± *x* ·$_r$ (*1*$_r$ ± −$_a$ *x*))^-*K*)))
⟨*proof*⟩

lemma (**in** *Corps*) *OstrowskiTr10*:⟦*valuation K v*; *x* ∈ *carrier K*;
¬ *0* ≤ *v x*⟧ ⟹ *0* < (*v* (*x* ·$_r$ ((*1*$_r$ ± *x* ·$_r$ (*1*$_r$ ± −$_a$ *x*))^-*K*)))
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-first*:*vals-nonequiv K* (*Suc 0*) *vv*
⟹ ∃ *x*∈*carrier K*. *Ostrowski-elem K* (*Suc 0*) *vv x*
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski*:∀ *vv*. *vals-nonequiv K* (*Suc n*) *vv* ⟶
(∃ *x*∈*carrier K*. *Ostrowski-elem K* (*Suc n*) *vv x*)
⟨*proof*⟩

lemma (**in** *Corps*) *val-1-nonzero*:⟦*valuation K v*; *x* ∈ *carrier K*; *v x* = *1*⟧ ⟹
x ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *Approximation1-5Tr1*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
n-val K (*vv 0*) = *vv 0*; *a* ∈ *carrier K*; *vv 0 a* = *1*; *x* ∈ *carrier K*;
Ostrowski-elem K (*Suc n*) *vv x*⟧ ⟹
∀ *m*. *2* ≤ *m* ⟶ *vv 0* ((*1*$_r$ ± −$_a$ *x*)^*K m* ± *a* ·$_r$ (*x*^*K m*)) = *1*
⟨*proof*⟩

lemma (**in** *Corps*) *Approximation1-5Tr3*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
x ∈ *carrier K*; *Ostrowski-elem K* (*Suc n*) *vv x*; *j* ∈ *nset* (*Suc 0*) (*Suc n*)⟧
⟹ *vv j* ((*1*$_r$ ± −$_a$ *x*)^*K m*) = *0*
⟨*proof*⟩

lemma (**in** *Corps*) *Approximation1-5Tr4*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
aa ∈ *carrier K*; *x* ∈ *carrier K*;
Ostrowski-elem K (*Suc n*) *vv x*; *j* ≤ (*Suc n*)⟧ ⟹
vv j (*aa* ·$_r$ (*x*^*K m*)) = *vv j aa* + (*int m*) ∗$_a$ (*vv j x*)
⟨*proof*⟩

lemma (**in** *Corps*) *Approximation1-5Tr5*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
a ∈ *carrier K*; *a* ≠ **0**; *x* ∈ *carrier K*;
Ostrowski-elem K (*Suc n*) *vv x*; *j* ∈ *nset* (*Suc 0*) (*Suc n*)⟧ ⟹
∃ *l*. ∀ *m*. *l* < *m* ⟶ *0* < (*vv j* (*a* ·$_r$ (*x*^*K m*)))
⟨*proof*⟩

lemma (**in** *Corps*) *Approximation1-5Tr6*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
a ∈ *carrier K*; *a* ≠ **0**; *x* ∈ *carrier K*;
Ostrowski-elem K (*Suc n*) *vv x*; *j* ∈ *nset* (*Suc 0*) (*Suc n*)⟧ ⟹

$\exists\, l.\ \forall\, m.\ l < m \longrightarrow vv\ j\ ((1_r \pm -_a\ x)^{\frown K\ m} \pm a \cdot_r (x^{\frown K\ m})) = 0$
⟨*proof*⟩

lemma (**in** *Corps*) *Approximation1-5Tr7*:⟦$a \in$ *carrier* K; *vv* 0 a = 1;
$x \in$ *carrier* K⟧ ⟹
vals-nonequiv K (*Suc* n) *vv* ∧ *Ostrowski-elem* K (*Suc* n) *vv* x ⟶
(∃ l. ∀ m. $l < m$ ⟶ (∀ j∈*nset* (*Suc* 0) (*Suc* n).
(*vv* j $((1_r \pm -_a\ x)^{\frown K\ m} \pm a \cdot_r (x^{\frown K\ m})) = 0$)))
⟨*proof*⟩

lemma (**in** *Corps*) *Approximation1-5P*:⟦*vals-nonequiv* K (*Suc* n) *vv*;
n-val K (*vv* 0) = *vv* 0⟧ ⟹
∃ x∈*carrier* K. ((*vv* 0 x = 1) ∧ (∀ j∈*nset* (*Suc* 0) (*Suc* n). (*vv* j x) = 0))
⟨*proof*⟩

lemma *K-gamma-hom*:$k \le n$ ⟹ ∀ $j \le n$. ($\lambda l.\ \gamma_{k\ l}$) $j \in$ *Zset*
⟨*proof*⟩

lemma *transpos-eq*:$(\tau_{0\ 0})\ k = k$
⟨*proof*⟩

lemma (**in** *Corps*) *transpos-vals-nonequiv*:⟦*vals-nonequiv* K (*Suc* n) *vv*;
$j \le$ (*Suc* n)⟧ ⟹ *vals-nonequiv* K (*Suc* n) (*vv* ∘ $(\tau_{0\ j})$)
⟨*proof*⟩

definition
Ostrowski-base :: [-, *nat* ⇒ 'b ⇒ *ant*, *nat*] ⇒ (*nat* ⇒ 'b)
((Ω_ _ _) [90,90,91]90) **where**
Ostrowski-base K *vv* n = (λj∈{h. $h \le n$}. (*SOME* x. x∈*carrier* K ∧
(*Ostrowski-elem* K n (*vv* ∘ $(\tau_{0\ j})$) x)))

definition
App-base :: [-, *nat* ⇒ 'b ⇒ *ant*, *nat*] ⇒ (*nat* ⇒ 'b) **where**
App-base K *vv* n = (λj∈{h. $h \le n$}. (*SOME* x. x∈*carrier* K ∧ (((*vv* ∘ $\tau_{0\ j}$) 0 x
= 1) ∧ (∀ k∈*nset* (*Suc* 0) n. ((*vv* ∘ $\tau_{0\ j}$) k x) = 0))))

lemma (**in** *Corps*) *Ostrowski-base-hom*:*vals-nonequiv* K (*Suc* n) *vv* ⟹
Ostrowski-base K *vv* (*Suc* n) ∈ {h. $h \le$ (*Suc* n)} → *carrier* K
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-base-mem*:*vals-nonequiv* K (*Suc* n) *vv* ⟹
∀ $j \le$ (*Suc* n). *Ostrowski-base* K *vv* (*Suc* n) $j \in$ *carrier* K
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-base-mem-1*:⟦*vals-nonequiv* K (*Suc* n) *vv*;
$j \le$ (*Suc* n)⟧ ⟹ *Ostrowski-base* K *vv* (*Suc* n) $j \in$ *carrier* K
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-base-nonzero*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
$j \leq$ *Suc n*⟧ $\Longrightarrow$ $(\Omega_{K\ vv\ (Suc\ n)})\ j \neq \mathbf{0}$
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-base-pos*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
$j \leq$ *Suc n*; *ja* $\leq$ *Suc n*; *ja* $\neq$ *j*⟧ $\Longrightarrow$ *0* $<$ ((*vv j*) $((\Omega_{K\ vv\ (Suc\ n)})\ ja)$)
⟨*proof*⟩

lemma (**in** *Corps*) *App-base-hom*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
$\forall j \leq$ (*Suc n*). *n-val K* (*vv j*) = *vv j*⟧ $\Longrightarrow$
$\forall j \leq$ (*Suc n*). *App-base K vv* (*Suc n*) *j* $\in$ *carrier K*
⟨*proof*⟩

lemma (**in** *Corps*) *Approzimation1-5P2*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
$\forall l \in \{h.\ h \leq$ *Suc n*$\}$. *n-val K* (*vv l*) = *vv l*; *i* $\leq$ *Suc n*; *j* $\leq$ *Suc n*⟧
$\Longrightarrow$ *vv i* (*App-base K vv* (*Suc n*) *j*) = $\delta_{i\ j}$
⟨*proof*⟩

lemma (**in** *Corps*) *Approximation1-5*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
$\forall j \leq$ (*Suc n*). *n-val K* (*vv j*) = *vv j*⟧ $\Longrightarrow$
$\exists x.\ (\forall j \leq$ (*Suc n*). *x j* $\in$ *carrier K*$) \wedge (\forall i \leq$ (*Suc n*). $\forall j \leq$ (*Suc n*).
((*vv i*) (*x j*) = $\delta_{i\ j}$))
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-baseTr0*:⟦*vals-nonequiv K* (*Suc n*) *vv*; *l* $\leq$ (*Suc n*) ⟧
$\Longrightarrow$ *0* $<$ ((*vv l*) ($1_r \pm -_a$ (*Ostrowski-base K vv* (*Suc n*) *l*))) $\wedge$
$(\forall m \in \{h.\ h \leq$ (*Suc n*)$\} - \{l\}$. *0* $<$ ((*vv m*) (*Ostrowski-base K vv* (*Suc n*) *l*)))
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-baseTr1*:⟦*vals-nonequiv K* (*Suc n*) *vv*; *l* $\leq$ (*Suc n*)⟧
$\Longrightarrow$ *0* $<$ ((*vv l*) ($1_r \pm -_a$ (*Ostrowski-base K vv* (*Suc n*) *l*)))
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-baseTr2*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
l $\leq$ (*Suc n*); *m* $\leq$ (*Suc n*); *l* $\neq$ *m*⟧ $\Longrightarrow$
0 $<$ ((*vv m*) (*Ostrowski-base K vv* (*Suc n*) *l*))
⟨*proof*⟩

lemma *Nset-have-two*:*j* $\in \{h.\ h \leq$ (*Suc n*)$\} \Longrightarrow \exists m \in \{h.\ h \leq$ (*Suc n*)$\}$. *j* $\neq$ *m*
⟨*proof*⟩

lemma (**in** *Corps*) *Ostrowski-base-npow-not-one*:⟦*0* $<$ *N*; *j* $\leq$ *Suc n*;
vals-nonequiv K (*Suc n*) *vv*⟧ $\Longrightarrow$
$1_r \pm -_a$ $((\Omega_{K\ vv\ (Suc\ n)})\ j^{\frown K\ N}) \neq \mathbf{0}$
⟨*proof*⟩

abbreviation

$CHOOSE :: [nat,\ nat] \Rightarrow nat\ \ ((\_C\_)\ [80,\ 81]80)$ **where**
${}_nC_i == n\ choose\ i$

lemma (**in** *Ring*) *expansion-of-sum1*:$x \in carrier\ R \Longrightarrow$
$(1_r \pm x)^{\frown R\ n} = nsum\ R\ (\lambda i.\ {}_nC_i \times_R x^{\frown R\ i})\ n$
⟨*proof*⟩

lemma (**in** *Ring*) *tail-of-expansion*:$x \in carrier\ R \Longrightarrow (1_r \pm x)^{\frown R\ (Suc\ n)} =$
$(nsum\ R\ (\lambda\ i.\ ({}_{(Suc\ n)}C_{(Suc\ i)} \times_R x^{\frown R\ (Suc\ i)}))\ n) \pm 1_r$
⟨*proof*⟩

lemma (**in** *Ring*) *tail-of-expansion1*:$x \in carrier\ R \Longrightarrow$
$(1_r \pm x)^{\frown R\ (Suc\ n)} = x \cdot_r (nsum\ R\ (\lambda\ i.\ ({}_{(Suc\ n)}C_{(Suc\ i)} \times_R x^{\frown R\ i}))\ n) \pm 1_r$
⟨*proof*⟩

lemma (**in** *Corps*) *nsum-in-VrTr*:$valuation\ K\ v \Longrightarrow$
$(\forall j \le n.\ f\ j \in carrier\ K) \wedge (\forall j \le n.$
$0 \le (v\ (f\ j))) \longrightarrow (nsum\ K\ f\ n) \in carrier\ (Vr\ K\ v)$
⟨*proof*⟩

lemma (**in** *Corps*) *nsum-in-Vr*:$[\![valuation\ K\ v;\ \forall j \le n.\ f\ j \in carrier\ K;$
$\forall j \le n.\ \ 0 \le (v\ (f\ j))]\!] \Longrightarrow (nsum\ K\ f\ n) \in carrier\ (Vr\ K\ v)$
⟨*proof*⟩

lemma (**in** *Corps*) *nsum-mem-in-Vr*:$[\![valuation\ K\ v;$
$\forall j \le n.\ (f\ j) \in carrier\ K;\ \forall j \le n.\ 0 \le (v\ (f\ j))]\!] \Longrightarrow$
$(nsum\ K\ f\ n) \in carrier\ (Vr\ K\ v)$
⟨*proof*⟩

lemma (**in** *Corps*) *val-nscal-ge-selfTr*:$[\![valuation\ K\ v;\ x \in carrier\ K;\ 0 \le v\ x]\!]$
$\Longrightarrow\ \ v\ x \le\ \ v\ (n \times_K x)$
⟨*proof*⟩

lemma (**in** *Corps*) *ApproximationTr*:$[\![valuation\ K\ v;\ x \in carrier\ K;\ 0 \le (v\ x)]\!]$
$\Longrightarrow$
$v\ x \le (v\ (1_r \pm -_a\ ((1_r \pm x)^{\frown K\ (Suc\ n)})))$
⟨*proof*⟩

lemma (**in** *Corps*) *ApproximationTr0*:$aa \in carrier\ K \Longrightarrow$
$(1_r \pm -_a\ (aa^{\frown K\ N}))^{\frown K\ N} \in carrier\ K$
⟨*proof*⟩

lemma (**in** *Corps*) *ApproximationTr1*:$aa \in carrier\ K \Longrightarrow$
$1_r \pm -_a\ ((1_r \pm -_a\ (aa^{\frown K\ N}))^{\frown K\ N}) \in carrier\ K$
⟨*proof*⟩

lemma (**in** *Corps*) *ApproximationTr2*:$[\![valuation\ K\ v;\ aa \in carrier\ K;\ aa \neq \mathbf{0};$
$0 \le (v\ aa)]\!] \Longrightarrow (int\ N) *_a (v\ aa) \le (v\ (1_r \pm -_a\ ((1_r \pm -_a\ (aa^{\frown K\ N}))^{\frown K\ N})))$

⟨*proof*⟩

lemma (**in** *Corps*) *eSum-tr*:
$(\ \forall j \leq n.\ (x\ j) \in \mathit{carrier}\ K) \wedge$
$(\ \forall j \leq n.\ (b\ j) \in \mathit{carrier}\ K) \wedge l \leq n \wedge$
$(\ \forall j{\in}(\{h.\ h \leq n\} - \{l\}).\ (g\ j = (x\ j) \cdot_r (1_r \pm -_a\ (b\ j)))) \wedge$
$g\ l = (x\ l) \cdot_r (-_a\ (b\ l))$
$\longrightarrow (\mathit{nsum}\ K\ (\lambda j \in \{h.\ h \leq n\}.\ (x\ j) \cdot_r (1_r \pm -_a\ (b\ j)))\ n) \pm (-_a\ (x\ l)) =$
$\mathit{nsum}\ K\ g\ n$
⟨*proof*⟩

lemma (**in** *Corps*) *eSum-minus-x*:$[\![\forall j \leq n.\ (x\ j) \in \mathit{carrier}\ K;$
$\forall j \leq n.\ (b\ j) \in \mathit{carrier}\ K;\ l \leq n;$
$\forall j{\in}(\{h.\ h \leq n\} - \{l\}).\ (g\ j = (x\ j) \cdot_r (1_r \pm -_a\ (b\ j)));$
$g\ l = (x\ l) \cdot_r (-_a\ (b\ l))\ ]\!] \Longrightarrow$
$(\mathit{nsum}\ K\ (\lambda j{\in}\{h.\ h \leq n\}.\ (x\ j) \cdot_r (1_r \pm -_a\ (b\ j)))\ n) \pm (-_a\ (x\ l)) =$
$\mathit{nsum}\ K\ g\ n$
⟨*proof*⟩

lemma (**in** *Ring*) *one-m-x-times*:$x \in \mathit{carrier}\ R \Longrightarrow$
$(1_r \pm -_a\ x) \cdot_r (\mathit{nsum}\ R\ (\lambda j.\ x^{\frown R}\ j)\ n) = 1_r \pm -_a\ (x^{\frown R}\ (\mathit{Suc}\ n))$
⟨*proof*⟩

lemma (**in** *Corps*) *x-pow-fSum-in-Vr*:$[\![\mathit{valuation}\ K\ v;\ x \in \mathit{carrier}\ (\mathit{Vr}\ K\ v)]\!] \Longrightarrow$
$(\mathit{nsum}\ K\ (\mathit{npow}\ K\ x)\ n) \in \mathit{carrier}\ (\mathit{Vr}\ K\ v)$
⟨*proof*⟩

lemma (**in** *Corps*) *val-1mx-pos*:$[\![\mathit{valuation}\ K\ v;\ x \in \mathit{carrier}\ K;$
$0 < (v\ (1_r \pm -_a\ x))]\!] \Longrightarrow\ v\ x = 0$
⟨*proof*⟩

lemma (**in** *Corps*) *val-1mx-pow*:$[\![\mathit{valuation}\ K\ v;\ x \in \mathit{carrier}\ K;$
$0 < (v\ (1_r \pm -_a\ x))]\!] \Longrightarrow 0 < (v\ (1_r \pm -_a\ x^{\frown K\ (\mathit{Suc}\ n)}))$
⟨*proof*⟩

lemma (**in** *Corps*) *ApproximationTr3*:$[\![\mathit{vals-nonequiv}\ K\ (\mathit{Suc}\ n)\ vv;$
$\forall l \leq (\mathit{Suc}\ n).\ x\ l \in \mathit{carrier}\ K;\ j \leq (\mathit{Suc}\ n)]\!] \Longrightarrow$
$\exists L.(\forall N.\ L < N \longrightarrow (\mathit{an}\ m) \leq (vv\ j\ ((\Sigma_e\ K\ (\lambda k{\in}\{h.\ h \leq (\mathit{Suc}\ n)\}.$
$(x\ k) \cdot_r (1_r \pm -_a\ (((1_r \pm -_a\ (((\Omega_{K\ vv\ (\mathit{Suc}\ n)})\ k)^{\frown K\ N}))^{\frown K\ N})))$
$(\mathit{Suc}\ n)) \pm -_a\ (x\ j))))$
⟨*proof*⟩

definition
$\mathit{app\text{-}lb} :: [\text{-}\ ,\ \mathit{nat},\ \mathit{nat} \Rightarrow 'b \Rightarrow \mathit{ant},\ \mathit{nat} \Rightarrow 'b,\ \mathit{nat}] \Rightarrow$
$(\mathit{nat} \Rightarrow \mathit{nat})\quad ((5\Psi\_\_\_\_\_)\ [98,98,98,98,99]98)$ **where**
$\Psi_{K\ n\ vv\ x\ m} = (\lambda j{\in}\{h.\ h \leq n\}.\ (\mathit{SOME}\ L.\ (\forall N.\ L < N \longrightarrow$
$(\mathit{an}\ m) \leq (vv\ j\ (\Sigma_e\ K\ (\lambda j{\in}\{h.\ h \leq n\}.\ (x\ j) \cdot_{r K} (1_{r K} \pm_K -_{a K}$
$(1_{r K} \pm_K -_{a K}\ ((\Omega_{K\ vv\ n})\ j)^{\frown K\ N})^{\frown K\ N}))\ n \pm_K -_{a K}\ (x\ j))))))$

lemma (**in** *Corps*) *app-LB*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
∀ *l*≤ (*Suc n*). *x l* ∈ *carrier K*; *j* ≤ (*Suc n*)⟧ ⟹
∀ *N*. (Ψ$_{K\ (Suc\ n)\ vv\ x\ m}$) *j* < *N* ⟶ (*an m*) ≤
(*vv j* (Σ$_e$ *K* (λ*j*∈{*h*. *h* ≤ (*Suc n*)}. (*x j*) ·$_r$ (1$_r$ ± −$_a$ (1$_r$ ±
−$_a$ ((Ω$_{K\ vv\ (Suc\ n)}$) *j*)$^{\frown K\ N}$)$^{\frown K\ N}$)) (*Suc n*) ± −$_a$ (*x j*)))
⟨*proof*⟩

lemma (**in** *Corps*) *ApplicationTr4*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
∀ *j*∈{*h*. *h* ≤ (*Suc n*)}. *x j* ∈ *carrier K*⟧ ⟹
∃ *l*. ∀ *N*. *l* < *N* ⟶ (∀ *j* ≤ (*Suc n*). (*an m*) ≤
(*vv j* (Σ$_e$ *K* (λ*j*∈{*h*. *h* ≤ (*Suc n*)}. (*x j*) ·$_r$ (1$_r$ ± −$_a$ (1$_r$ ±
−$_a$ ((Ω$_{K\ vv\ (Suc\ n)}$) *j*)$^{\frown K\ N}$)$^{\frown K\ N}$)) (*Suc n*) ± −$_a$ (*x j*))))
⟨*proof*⟩

theorem (**in** *Corps*) *Approximation-thm*:⟦*vals-nonequiv K* (*Suc n*) *vv*;
∀ *j*≤ (*Suc n*). (*x j*) ∈ *carrier K*⟧ ⟹
∃ *y*∈*carrier K*. ∀ *j*≤ (*Suc n*). (*an m*) ≤ (*vv j* (*y* ± −$_a$ (*x j*)))
⟨*proof*⟩

definition
distinct-pds :: [-, *nat*, *nat* ⇒ (′*b* ⇒ *ant*) *set*] ⇒ *bool* **where**
distinct-pds K n P ⟷ (∀ *j*≤ *n*. *P j* ∈ *Pds* $_K$) ∧
(∀ *l*≤ *n*. ∀ *m*≤ *n*. *l* ≠ *m* ⟶ *P l* ≠ *P m*)

lemma (**in** *Corps*) *distinct-pds-restriction*:⟦*distinct-pds K* (*Suc n*) *P*⟧ ⟹
distinct-pds K n P
⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-distinct-prime-divisors*:*distinct-pds K n P* ⟹
Ring (*Sr K* {*x*. *x*∈*carrier K* ∧ (∀ *j*≤ *n*. 0 ≤ ((ν $_{K\ (P\ j)}$) *x*))})
⟨*proof*⟩

lemma (**in** *Corps*) *distinct-pds-valuation*:⟦*j* ≤ (*Suc n*);
distinct-pds K (*Suc n*) *P*⟧ ⟹ *valuation K* (ν$_{K\ (P\ j)}$)
⟨*proof*⟩

lemma (**in** *Corps*) *distinct-pds-valuation1*:⟦0 < *n*; *j* ≤ *n*; *distinct-pds K n P*⟧
⟹ *valuation K* (ν$_{K\ (P\ j)}$)
⟨*proof*⟩

lemma (**in** *Corps*) *distinct-pds-valuation2*:⟦*j* ≤ *n*; *distinct-pds K n P*⟧ ⟹
valuation K (ν$_{K\ (P\ j)}$)
⟨*proof*⟩

definition
ring-n-pd :: [(′*b*, ′*m*) *Ring-scheme*, *nat* ⇒ (′*b* ⇒ *ant*) *set*,

$nat\ ] \Rightarrow ('b,\ 'm)\ Ring\text{-}scheme$
$((3O\_\ \_\ \_)\ [98,98,99]98)$ **where**
$O_{K\ P\ n} = Sr\ K\ \{x.\ x \in carrier\ K \wedge$
$(\forall j \leq n.\ 0 \leq ((\nu_{K\ (P\ j)})\ x))\}$

lemma (**in** *Corps*) *ring-n-pd*:*distinct-pds K n P* $\Longrightarrow$ *Ring* $(O_{K\ P\ n})$
⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-pd-Suc*:*distinct-pds K* (*Suc n*) *P* $\Longrightarrow$
carrier $(O_{K\ P\ (Suc\ n)}) \subseteq$ *carrier* $(O_{K\ P\ n})$
⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-pd-pOp-K-pOp*:⟦*distinct-pds K n P*; *x*∈*carrier* $(O_{K\ P\ n})$;
$y \in$ *carrier* $(O_{K\ P\ n})$⟧ $\Longrightarrow x \pm_{(O_{K\ P\ n})} y = x \pm y$
⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-pd-tOp-K-tOp*:⟦*distinct-pds K n P*; *x* ∈*carrier* $(O_{K\ P\ n})$;
y ∈ *carrier* $(O_{K\ P\ n})$⟧ $\Longrightarrow$ $x \cdot_{r(O_{K\ P\ n})} y = x \cdot_r y$
⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-eSum-K-eSumTr*:*distinct-pds K n P* $\Longrightarrow$
$(\forall j \leq m.\ f\ j \in carrier\ (O_{K\ P\ n})) \longrightarrow nsum\ (O_{K\ P\ n})\ f\ m = nsum\ K\ f\ m$
⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-eSum-K-eSum*:⟦*distinct-pds K n P*;
$\forall j \leq m.\ f\ j \in carrier\ (O_{K\ P\ n})$⟧ $\Longrightarrow nsum\ (O_{K\ P\ n})\ f\ m = nsum\ K\ f\ m$
⟨*proof*⟩

lemma (**in** *Corps*) *ideal-eSum-closed*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$\forall j \leq m.\ f\ j \in I$⟧ $\Longrightarrow$ $nsum\ K\ f\ m \in I$
⟨*proof*⟩

definition
prime-n-pd :: [-, *nat* ⇒ (*'b* ⇒ *ant*) *set*,
nat, *nat*] ⇒ *'b set*
$((4P\_\ \_\ \_\ -)\ [98,98,98,99]98)$ **where**
$P_{K\ P\ n}\ j = \{x.\ x \in (carrier\ (O_{K\ P\ n})) \wedge 0 < ((\nu_{K\ (P\ j)})\ x)\}$

lemma (**in** *Corps*) *zero-in-ring-n-pd-zero-K*:*distinct-pds K n P* $\Longrightarrow$
$\mathbf{0}_{(O_{K\ P\ n})} = \mathbf{0}_K$
⟨*proof*⟩

lemma (**in** *Corps*) *one-in-ring-n-pd-one-K*:*distinct-pds K n P* $\Longrightarrow$
$1_{r(O_{K\ P\ n})} = 1_r$
⟨*proof*⟩

lemma (**in** *Corps*) *mem-ring-n-pd-mem-K*:⟦*distinct-pds K n P*; *x* ∈*carrier* $(O_{K\ P\ n})$⟧

$\Longrightarrow x \in carrier\ K$
⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-tOp-K-tOp*:⟦*distinct-pds K n P*; $x \in carrier\ (O_{K\ P\ n})$;
$y \in carrier\ (O_{K\ P\ n})$⟧ $\Longrightarrow x \cdot_{r(O_{K\ P\ n})} y = x \cdot_r y$
⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-exp-K-exp*:⟦*distinct-pds K n P*; $x \in carrier\ (O_{K\ P\ n})$⟧
$\Longrightarrow x^{\frown K\ m} = x^{\frown (O_{K\ P\ n})\ m}$
⟨*proof*⟩

lemma (**in** *Corps*) *prime-n-pd-prime*:⟦*distinct-pds K n P*; $j \leq n$⟧ $\Longrightarrow$
prime-ideal $(O_{K\ P\ n})$ $(P_{K\ P\ n\ j})$
⟨*proof*⟩

lemma (**in** *Corps*) *n-eq-val-eq-idealTr*:
⟦*distinct-pds K n P*; $x \in carrier\ (O_{K\ P\ n})$; $y \in carrier\ (O_{K\ P\ n})$;
$\forall j \leq n.\ ((\nu_{K\ (P\ j)})\ x) \leq ((\nu_{K\ (P\ j)})\ y)$⟧ $\Longrightarrow$ *Rxa* $(O_{K\ P\ n})\ y \subseteq$ *Rxa* $(O_{K\ P\ n})\ x$
⟨*proof*⟩

lemma (**in** *Corps*) *n-eq-val-eq-ideal*:⟦*distinct-pds K n P*; $x \in carrier\ (O_{K\ P\ n})$;
$y \in carrier\ (O_{K\ P\ n})$; $\forall j \leq n.((\nu_{K\ (P\ j)})\ x) = ((\nu_{K\ (P\ j)})\ y)$⟧ $\Longrightarrow$
Rxa $(O_{K\ P\ n})\ x =$ *Rxa* $(O_{K\ P\ n})\ y$
⟨*proof*⟩

definition
mI-gen :: [- , *nat* ⇒ (′*r* ⇒ *ant*) *set*, *nat*, ′*r set*] ⇒ ′*r* **where**
mI-gen K P n I = (*SOME x*. $x \in I \wedge$
$(\forall j \leq n.\ (\nu_{K\ (P\ j)})\ x = LI\ K\ (\nu_{K\ (P\ j)})\ I)$)

definition
mL :: [-, *nat* ⇒ (′*r* ⇒ *ant*) *set*, ′*r set*, *nat*] ⇒ *int* **where**
mL K P I j = *tna* $(LI\ K\ (\nu_{K\ (P\ j)})\ I)$

lemma (**in** *Corps*) *mI-vals-nonempty*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})\ I$; $j \leq n$⟧
$\Longrightarrow (\nu_{K\ (P\ j)})\ `\ I \neq \{\}$
⟨*proof*⟩

lemma (**in** *Corps*) *mI-vals-LB*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})\ I$; $j \leq n$⟧ $\Longrightarrow$
$((\nu_{K\ (P\ j)})\ `I) \subseteq LBset\ (ant\ 0)$
⟨*proof*⟩

lemma (**in** *Corps*) *mL-hom*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})\ I$;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq carrier\ (O_{K\ P\ n})$⟧ $\Longrightarrow$
$\forall j \leq n.\ mL\ K\ P\ I\ j \in Zset$
⟨*proof*⟩

lemma (**in** *Corps*) *ex-Zleast-in-mI*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})\ I$; $j \leq n$⟧

$\Longrightarrow \exists x{\in}I.\ (\nu_{K\ (P\ j)})\ x = LI\ K\ (\nu_{K\ (P\ j)})\ I$
⟨*proof*⟩

lemma (**in** *Corps*) *val-LI-pos*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $j \leq n$⟧ $\Longrightarrow$ $0 \leq LI\ K\ (\nu_{K\ (P\ j)})\ I$
⟨*proof*⟩

lemma (**in** *Corps*) *val-LI-noninf*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $j \leq n$⟧ $\Longrightarrow$ $LI\ K\ (\nu_{K\ (P\ j)})\ I \neq \infty$
⟨*proof*⟩

lemma (**in** *Corps*) *Zleast-in-mI-pos*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $j \leq n$⟧ $\Longrightarrow$ $0 \leq mL\ K\ P\ I\ j$
⟨*proof*⟩

lemma (**in** *Corps*) *Zleast-mL-I*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $j \leq n$;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $x \in I$⟧ $\Longrightarrow$ $ant\ (mL\ K\ P\ I\ j) \leq ((\nu_{K\ (P\ j)})\ x)$
⟨*proof*⟩

lemma (**in** *Corps*) *Zleast-LI*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $j \leq n$;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $x \in I$⟧ $\Longrightarrow$ $(LI\ K\ (\nu_{K\ (P\ j)})\ I) \leq ((\nu_{K\ (P\ j)})\ x)$
⟨*proof*⟩

lemma (**in** *Corps*) *mpdiv-vals-nonequiv*:*distinct-pds K n P* $\Longrightarrow$
vals-nonequiv K n $(\lambda j.\ \nu_{K\ (P\ j)})$
⟨*proof*⟩

definition
KbaseP :: [-, *nat* ⇒ (′*r* ⇒ *ant*) *set*, *nat*] ⇒
(*nat* ⇒ ′*r*) ⇒ *bool* **where**
KbaseP K P n f ⟷ $(\forall j \leq n.\ f\ j \in carrier\ K) \wedge$
$(\forall j \leq n.\ \forall l \leq n.\ (\nu_{K\ (P\ j)})\ (f\ l) = (\delta_{j\ l}))$

definition
Kbase :: [-, *nat*, *nat* ⇒ (′*r* ⇒ *ant*) *set*]
⇒ (*nat* ⇒ ′*r*) ((*3Kb*_ _ _) [*95*,*95*,*96*]*95*) **where**
$Kb_{K\ n\ P} = (SOME\ f.\ KbaseP\ K\ P\ n\ f)$

lemma (**in** *Corps*) *KbaseTr*:*distinct-pds K n P* $\Longrightarrow$ $\exists f.\ KbaseP\ K\ P\ n\ f$
⟨*proof*⟩

lemma (**in** *Corps*) *KbaseTr1*:*distinct-pds K n P* $\Longrightarrow$ $KbaseP\ K\ P\ n\ (Kb_{K\ n\ P})$
⟨*proof*⟩

lemma (**in** *Corps*) *Kbase-hom*:*distinct-pds K n P* $\Longrightarrow$
$\forall j \leq n.\ (Kb_{K\ n\ P})\ j \in carrier\ K$
⟨*proof*⟩

lemma (**in** *Corps*) *Kbase-Kronecker*:*distinct-pds K n P* $\Longrightarrow$
$\forall j \leq n.\ \forall l \leq n.\ (\nu_{K\ (P\ j)})\ ((Kb_{K\ n\ P})\ l) = \delta_{j\ l}$
⟨*proof*⟩

lemma (**in** *Corps*) *Kbase-nonzero*:*distinct-pds K n P* $\Longrightarrow$
$\forall j \leq n.\ (Kb_{K\ n\ P})\ j \neq \mathbf{0}$
⟨*proof*⟩

lemma (**in** *Corps*) *Kbase-hom1*:*distinct-pds K n P* $\Longrightarrow$
$\forall j \leq n.\ (Kb_{K\ n\ P})\ j \in carrier\ K - \{\mathbf{0}\}$
⟨*proof*⟩

definition
Zl-mI :: [-, *nat* ⇒ ('*b* ⇒ *ant*) *set*, '*b set*]
⇒ *nat* ⇒ '*b* **where**
Zl-mI K P I j = (*SOME x*. ($x \in I \wedge (\ (\nu_{K\ (P\ j)})\ x = LI\ K\ (\nu_{K\ (P\ j)})\ I)$))

lemma (**in** *Corps*) *value-Zl-mI*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $j \leq n$⟧
$\Longrightarrow$ (*Zl-mI K P I j* ∈ *I*) ∧ $(\nu_{K\ (P\ j)})$ (*Zl-mI K P I j*) = *LI K* $(\nu_{K\ (P\ j)})$ *I*
⟨*proof*⟩

lemma (**in** *Corps*) *Zl-mI-nonzero*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $j \leq n$⟧ $\Longrightarrow$ *Zl-mI K P I j* ≠ **0**
⟨*proof*⟩

lemma (**in** *Corps*) *Zl-mI-mem-K*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $l \leq n$⟧
$\Longrightarrow$ (*Zl-mI K P I l*) ∈ *carrier K*
⟨*proof*⟩

definition
mprod-exp :: [-, *nat* ⇒ *int*, *nat* ⇒ '*b*, *nat*]
⇒ '*b* **where**
mprod-exp K e f n = *nprod K* $(\lambda j.\ ((f\ j)_K{}^{(e\ j)}))$ *n*

lemma (**in** *Corps*) *mprod-expR-memTr*:($\forall j \leq n.\ f\ j \in carrier\ K$) ⟶
mprod-expR K e f n ∈ *carrier K*
⟨*proof*⟩

lemma (**in** *Corps*) *mprod-expR-mem*:$\forall j \leq n.\ f\ j \in carrier\ K \Longrightarrow$
mprod-expR K e f n ∈ *carrier K*
⟨*proof*⟩

lemma (**in** *Corps*) *mprod-Suc*:⟦ $\forall j \leq (Suc\ n).\ e\ j \in Zset$;
$\forall j \leq (Suc\ n).\ f\ j \in (carrier\ K - \{\mathbf{0}\})$⟧ $\Longrightarrow$
mprod-exp K e f (*Suc n*) = (*mprod-exp K e f n*) $\cdot_r$ $((f\ (Suc\ n))_K{}^{(e\ (Suc\ n))})$
⟨*proof*⟩

lemma (**in** *Corps*) *mprod-memTr*:

$(\forall j \leq n.\ e\ j \in Zset) \wedge (\forall j \leq n.\ f\ j \in ((carrier\ K) - \{\mathbf{0}\})) \longrightarrow$
$(mprod\text{-}exp\ K\ e\ f\ n) \in ((carrier\ K) - \{\mathbf{0}\})$
⟨*proof*⟩

lemma (**in** *Corps*) *mprod-mem*:⟦$\forall j \leq n.\ e\ j \in Zset$; $\forall j \leq n.\ f\ j \in ((carrier\ K) - \{\mathbf{0}\})$⟧ $\Longrightarrow$ $(mprod\text{-}exp\ K\ e\ f\ n) \in ((carrier\ K) - \{\mathbf{0}\})$
⟨*proof*⟩

lemma (**in** *Corps*) *mprod-mprodR*:⟦$\forall j \leq n.\ e\ j \in Zset$; $\forall j \leq n.\ 0 \leq (e\ j)$; $\forall j \leq n.\ f\ j \in ((carrier\ K) - \{\mathbf{0}\})$⟧ $\Longrightarrow$
$mprod\text{-}exp\ K\ e\ f\ n = mprod\text{-}expR\ K\ (nat\ o\ e)\ f\ n$
⟨*proof*⟩

2.8.1 Representation of an ideal I as a product of prime ideals

lemma (**in** *Corps*) *ring-n-mprod-mprodRTr*:*distinct-pds K n P* $\Longrightarrow$
$(\forall j \leq m.\ e\ j \in Zset) \wedge (\forall j \leq m.\ 0 \leq (e\ j)) \wedge$
$(\forall j \leq m.\ f\ j \in carrier\ (O_{K\ P\ n}) - \{\mathbf{0}_{(O_{K\ P\ n})}\}) \longrightarrow$
$mprod\text{-}exp\ K\ e\ f\ m = mprod\text{-}expR\ (O_{K\ P\ n})\ (nat\ o\ e)\ f\ m$
⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-mprod-mprodR*:⟦*distinct-pds K n P*; $\forall j \leq m.\ e\ j \in Zset$; $\forall j \leq m.\ 0 \leq (e\ j)$; $\forall j \leq m.\ f\ j \in carrier\ (O_{K\ P\ n}) - \{\mathbf{0}_{(O_{K\ P\ n})}\}$⟧
$\Longrightarrow$ $mprod\text{-}exp\ K\ e\ f\ m = mprod\text{-}expR\ (O_{K\ P\ n})\ (nat\ o\ e)\ f\ m$
⟨*proof*⟩

lemma (**in** *Corps*) *value-mprod-expTr*:*valuation K v* $\Longrightarrow$
$(\forall j \leq n.\ e\ j \in Zset) \wedge (\forall j \leq n.\ f\ j \in (carrier\ K - \{\mathbf{0}\})) \longrightarrow$
$v\ (mprod\text{-}exp\ K\ e\ f\ n) = ASum\ (\lambda j.\ (e\ j) *_a (v\ (f\ j)))\ n$
⟨*proof*⟩

lemma (**in** *Corps*) *value-mprod-exp*:⟦*valuation K v*; $\forall j \leq n.\ e\ j \in Zset$; $\forall j \leq n.\ f\ j \in (carrier\ K - \{\mathbf{0}\})$⟧ $\Longrightarrow$
$v\ (mprod\text{-}exp\ K\ e\ f\ n) = ASum\ (\lambda j.\ (e\ j) *_a (v\ (f\ j)))\ n$
⟨*proof*⟩

lemma (**in** *Corps*) *mgenerator0-1*:⟦*distinct-pds K (Suc n) P*; *ideal* $(O_{K\ P\ (Suc\ n)})\ I$; $I \neq \{\mathbf{0}_{(O_{K\ P\ (Suc\ n)})}\}$; $I \neq carrier\ (O_{K\ P\ (Suc\ n)})$; $j \leq (Suc\ n)$⟧ $\Longrightarrow$
$((\nu_{K\ (P\ j)})\ (mprod\text{-}exp\ K\ (mL\ K\ P\ I)\ (Kb_{K\ (Suc\ n)\ P})\ (Suc\ n))) =$
$((\nu_{K\ (P\ j)})\ (Zl\text{-}mI\ K\ P\ I\ j))$
⟨*proof*⟩

lemma (**in** *Corps*) *mgenerator0-2*:⟦ $0 < n$; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})\ I$; $I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq carrier\ (O_{K\ P\ n})$; $j \leq n$⟧ $\Longrightarrow$
$((\nu_{K\ (P\ j)})\ (mprod\text{-}exp\ K\ (mL\ K\ P\ I)\ (Kb_{K\ n\ P})\ n)) = ((\nu_{K\ (P\ j)})\ (Zl\text{-}mI\ K\ P$

$I\ j))$
⟨*proof*⟩

lemma (**in** *Corps*) *mgenerator1*:⟦*distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq$ *carrier* $(O_{K\ P\ n})$; $j \leq n$⟧ ⟹
$((\nu_{K\ (P\ j)})\ (mprod\text{-}exp\ K\ (mL\ K\ P\ I)\ (Kb_{K\ n\ P})\ n)) = ((\nu_{K\ (P\ j)})\ (Zl\text{-}mI\ K\ P\ I\ j))$
⟨*proof*⟩

lemma (**in** *Corps*) *mgenerator2Tr1*:⟦$0 < n$; $j \leq n$; $k \leq n$; *distinct-pds K n P*⟧ ⟹
$(\nu_{K\ (P\ j)})\ (mprod\text{-}exp\ K\ (\lambda l.\ \gamma_{k\ l})\ (Kb_{K\ n\ P})\ n) = (\gamma_{k\ j}) *_a (\delta_{j\ j})$
⟨*proof*⟩

lemma (**in** *Corps*) *mgenerator2Tr2*:⟦$0 < n$; $j \leq n$; $k \leq n$; *distinct-pds K n P*⟧ ⟹
$(\nu_{K\ (P\ j)})\ ((mprod\text{-}exp\ K\ (\lambda l.\ \gamma_{k\ l})\ (Kb_{K\ n\ P})\ n)_K{}^m) = ant\ (m * (\gamma_{k\ j}))$

⟨*proof*⟩

lemma (**in** *Corps*) *mgenerator2Tr3-1*:⟦$0 < n$; $j \leq n$; $k \leq n$; $j = k$;
distinct-pds K n P⟧ ⟹
$(\nu_{K\ (P\ j)})\ ((mprod\text{-}exp\ K\ (\lambda l.\ (\gamma_{k\ l}))\ (Kb_{K\ n\ P})\ n)_K{}^m) = 0$
⟨*proof*⟩

lemma (**in** *Corps*) *mgenerator2Tr3-2*:⟦$0 < n$; $j \leq n$; $k \leq n$; $j \neq k$;
distinct-pds K n P⟧ ⟹
$(\nu_{K\ (P\ j)})\ ((mprod\text{-}exp\ K\ (\lambda l.\ (\gamma_{k\ l}))\ (Kb_{K\ n\ P})\ n)_K{}^m) = ant\ m$
⟨*proof*⟩

lemma (**in** *Corps*) *mgeneratorTr4*:⟦$0 < n$; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{O_{K\ P\ n}}\}$; $I \neq$ *carrier* $(O_{K\ P\ n})$⟧ ⟹
mprod-exp K $(mL\ K\ P\ I)$ $(Kb_{K\ n\ P})$ $n \in$ *carrier* $(O_{K\ P\ n})$
⟨*proof*⟩

definition
m-zmax-pdsI-hom :: [-, *nat* ⇒ ('*b* ⇒ *ant*) *set*, '*b set*] ⇒ *nat* ⇒ *int* **where**
m-zmax-pdsI-hom K P I = (λ*j*. *tna* (*AMin* $((\nu_{K\ (P\ j)})$ ‘ *I*)))

definition
m-zmax-pdsI :: [-, *nat*, *nat* ⇒ ('*b* ⇒ *ant*) *set*, '*b set*] ⇒ *int* **where**
m-zmax-pdsI K n P I = (*m-zmax n* (*m-zmax-pdsI-hom K P I*)) + *1*

lemma (**in** *Corps*) *value-Zl-mI-pos*:⟦$0 < n$; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq$ *carrier* $(O_{K\ P\ n})$; $j \leq n$; $l \leq n$⟧ ⟹
$0 \leq ((\nu_{K\ (P\ j)})\ (Zl\text{-}mI\ K\ P\ I\ l))$
⟨*proof*⟩

lemma (**in** *Corps*) *value-mI-genTr1*:⟦$0 < n$; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$
I;

$I \neq \{\mathbf{0}_{O_{K\ P\ n}}\}$; $I \neq carrier\ (O_{K\ P\ n})$; $j \leq n\rrbracket \Longrightarrow$
$(mprod\text{-}exp\ K\ (K\text{-}gamma\ j)\ (Kb_{K\ n\ P})\ n)_K{}^{(m\text{-}zmax\text{-}pdsI\ K\ n\ P\ I)} \in carrier\ K$
⟨*proof*⟩

lemma (**in** *Corps*) *value-mI-genTr1-0*:⟦$0 < n$; *distinct-pds K n P*;
ideal $(O_{K\ P\ n})$ *I*; $I \neq \{\mathbf{0}_{O_{K\ P\ n}}\}$; $I \neq carrier\ (O_{K\ P\ n})$; $j \leq n\rrbracket$
$\Longrightarrow (mprod\text{-}exp\ K\ (K\text{-}gamma\ j)\ (Kb_{K\ n\ P})\ n) \in carrier\ K$
⟨*proof*⟩

lemma (**in** *Corps*) *value-mI-genTr2*:⟦$0 < n$; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{O_{K\ P\ n}}\}$; $I \neq carrier\ (O_{K\ P\ n})$; $j \leq n\rrbracket \Longrightarrow$
$(mprod\text{-}exp\ K\ (K\text{-}gamma\ j)\ (Kb_{K\ n\ P})\ n)_K{}^{(m\text{-}zmax\text{-}pdsI\ K\ n\ P\ I)} \neq \mathbf{0}$
⟨*proof*⟩

lemma (**in** *Corps*) *value-mI-genTr3*:⟦$0 < n$; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{O_{K\ P\ n}}\}$; $I \neq carrier\ (O_{K\ P\ n})$; $j \leq n\rrbracket \Longrightarrow$
$(Zl\text{-}mI\ K\ P\ I\ j) \cdot_r ((mprod\text{-}exp\ K\ (K\text{-}gamma\ j)\ (Kb_{K\ n\ P})\ n)_K{}^{(m\text{-}zmax\text{-}pdsI\ K\ n\ P\ I)})$
$\in carrier\ K$
⟨*proof*⟩

lemma (**in** *Corps*) *value-mI-gen*:⟦$0 < n$; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq carrier\ (O_{K\ P\ n})$; $j \leq n\rrbracket \Longrightarrow$
$(\nu_{K\ (P\ j)})\ (nsum\ K\ (\lambda k.\ ((Zl\text{-}mI\ K\ P\ I\ k) \cdot_r ((mprod\text{-}exp\ K\ (\lambda l.\ (\gamma_{k\ l}))\ (Kb_{K\ n\ P})$
$n)_K{}^{(m\text{-}zmax\text{-}pdsI\ K\ n\ P\ I)}))\ n) = LI\ K\ (\nu_{K\ (P\ j)})\ I$
⟨*proof*⟩

lemma (**in** *Corps*) *mI-gen-in-I*:⟦$0 < n$; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq carrier\ (O_{K\ P\ n})\rrbracket \Longrightarrow$
$(nsum\ K\ (\lambda k.\ ((Zl\text{-}mI\ K\ P\ I\ k) \cdot_r$
$((mprod\text{-}exp\ K\ (\lambda l.\ (\gamma_{k\ l}))\ (Kb_{K\ n\ P})\ n)_K{}^{(m\text{-}zmax\text{-}pdsI\ K\ n\ P\ I)}))\ n) \in I$
⟨*proof*⟩

We write the element $e\Sigma\ K\ (\lambda k.\ (Zl\text{-}mI\ K\ P\ I\ k) \cdot_K ((mprod\text{-}exp\ K\ (K\text{-}gamma\ k)\ (Kb_{K\ n\ P})\ n)_K{}^{(}m\text{-}zmax\text{-}pdsI\ K\ n\ P\ I)))\ n$ as $mIg_{K\ G\ a\ i\ n\ P\ I}$

definition
$mIg :: [\text{-}, nat, nat \Rightarrow ('b \Rightarrow ant)\ set,$
$'b\ set] \Rightarrow 'b\ ((4mIg\ \_\ \_\ \_\ \_)\ [82,82,82,83]82)$ **where**
$mIg_{K\ n\ P\ I} = \Sigma_e\ K\ (\lambda k.\ (Zl\text{-}mI\ K\ P\ I\ k) \cdot_r K$
$((mprod\text{-}exp\ K\ (K\text{-}gamma\ k)\ (Kb_{K\ n\ P})\ n)_K{}^{(m\text{-}zmax\text{-}pdsI\ K\ n\ P\ I)}))\ n$

We can rewrite above two lemmas by using $mIg_{K\ G\ a\ i\ n\ P\ I}$

lemma (**in** *Corps*) *value-mI-gen1*:⟦$0 < n$; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*;
$I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq carrier\ (O_{K\ P\ n})\rrbracket \Longrightarrow$

$$\forall j \leq n.(\nu_{K\ (P\ j)})\ (mIg_{K\ n\ P\ I}) = LI\ K\ (\nu_{K\ (P\ j)})\ I$$

⟨*proof*⟩

lemma (**in** *Corps*) *mI-gen-in-I1*:⟦*0 < n*; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq$ *carrier* $(O_{K\ P\ n})$⟧ ⟹ $(mIg_{K\ n\ P\ I}) \in I$

⟨*proof*⟩

lemma (**in** *Corps*) *mI-principalTr*:⟦*0 < n*; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq$ *carrier* $(O_{K\ P\ n})$; $x \in I$⟧ ⟹
$\forall j \leq n.\ ((\nu_{K\ (P\ j)})\ (mIg_{K\ n\ P\ I})) \leq ((\nu_{K\ (P\ j)})\ x)$

⟨*proof*⟩

lemma (**in** *Corps*) *mI-principal*:⟦*0 < n*; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $I \neq \{\mathbf{0}_{(O_{K\ P\ n})}\}$; $I \neq$ *carrier* $(O_{K\ P\ n})$⟧ ⟹
$I = Rxa\ (O_{K\ P\ n})\ (mIg_{K\ n\ P\ I})$

⟨*proof*⟩

2.8.2 *prime-n-pd*

lemma (**in** *Corps*) *prime-n-pd-principal*:⟦*distinct-pds K n P*; $j \leq n$⟧ ⟹
$(P_{K\ P\ n}\ j) = Rxa\ (O_{K\ P\ n})\ (((Kb_{K\ n\ P})\ j))$

⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-prod-primesTr*:⟦*0 < n*; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $I \neq \{\mathbf{0}_{O_{K\ P\ n}}\}$; $I \neq$ *carrier* $(O_{K\ P\ n})$⟧ ⟹
$\forall j \leq n.(\nu_{K\ (P\ j)})\ (mprod\text{-}exp\ K\ (mL\ K\ P\ I)\ (Kb_{K\ n\ P})\ n) =$
$(\nu_{K\ (P\ j)})\ (mIg_{K\ n\ P\ I})$

⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-prod-primesTr1*:⟦*0 < n*; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $I \neq \{\mathbf{0}_{O_{K\ P\ n}}\}$; $I \neq$ *carrier* $(O_{K\ P\ n})$⟧ ⟹
$I = (O_{K\ P\ n})\ \diamondsuit_p\ (mprod\text{-}exp\ K\ (mL\ K\ P\ I)\ (Kb_{K\ n\ P})\ n)$

⟨*proof*⟩

lemma (**in** *Corps*) *ring-n-prod-primes*:⟦*0 < n*; *distinct-pds K n P*; *ideal* $(O_{K\ P\ n})$ *I*; $I \neq \{\mathbf{0}_{O_{K\ P\ n}}\}$; $I \neq$ *carrier* $(O_{K\ P\ n})$; $\forall k \leq n.\ J\ k = (P_{K\ P\ n}\ k)^{\diamondsuit(O_{K\ P\ n})\ (nat\ ((mL\ K\ P\ I)\ k))}$⟧ ⟹
$I = i\Pi_{(O_{K\ P\ n}),n}\ J$

⟨*proof*⟩

end

theory *Valuation3*
imports *Valuation2*
begin

2.9 Completion

In this section we formalize "completion" of the ground field K

definition
limit :: [-, 'b ⇒ *ant*, *nat* ⇒ 'b, 'b]
⇒ *bool* ((4*lim* _ _ - -) [90,90,90,91]90) **where**
$lim_{K\ v}\ f\ b \longleftrightarrow (\forall N.\ \exists M.\ (\forall n.\ M < n \longrightarrow$
$((f\ n) \pm_K (-_a K\ b)) \in (vp\ K\ v)\ ^{(Vr\ K\ v)\ (an\ N)}))$

lemma *not-in-singleton-noneq*:$x \notin \{a\} \Longrightarrow x \neq a$
⟨*proof*⟩

lemma *noneq-not-in-singleton*:$x \neq a \Longrightarrow x \notin \{a\}$
⟨*proof*⟩

lemma *inf-neq-1*[*simp*]:$\infty \neq 1$
⟨*proof*⟩

lemma *a1-neq-0*[*simp*]:$(1::ant) \neq 0$
⟨*proof*⟩

lemma *a1-poss*[*simp*]:$(0::ant) < 1$
⟨*proof*⟩

lemma *a-p1-gt*[*simp*]:$[\![a \neq \infty;\ a \neq -\infty]\!] \Longrightarrow a < a + 1$
⟨*proof*⟩

lemma (**in** *Corps*) *vpr-pow-inter-zero*:*valuation K v* ⟹
$(\bigcap \{I.\ \exists n.\ I = (vp\ K\ v)^{(Vr\ K\ v)\ (an\ n)}\}) = \{\mathbf{0}\}$
⟨*proof*⟩

lemma (**in** *Corps*) *limit-diff-n-val*:$[\![b \in carrier\ K;\ \forall j.\ f\ j \in carrier\ K;$
valuation K v$]\!] \Longrightarrow (lim_{K\ v}\ f\ b) = (\forall N.\ \exists M.\ \forall n.\ M < n \longrightarrow$
$(an\ N) \leq (n\text{-}val\ K\ v\ ((f\ n) \pm (-_a\ b))))$
⟨*proof*⟩

lemma (**in** *Corps*) *an-na-Lv*:*valuation K v* ⟹ $an\ (na\ (Lv\ K\ v)) = Lv\ K\ v$
⟨*proof*⟩

lemma (**in** *Corps*) *limit-diff-val*:$[\![b \in carrier\ K;\ \forall j.\ f\ j \in carrier\ K;$
valuation K v$]\!] \Longrightarrow (lim_{K\ v}\ f\ b) = (\forall N.\ \exists M.\ \forall n.\ M < n \longrightarrow$
$(an\ N) \leq (v\ ((f\ n) \pm (-_a\ b))))$
⟨*proof*⟩

uniqueness of the limit is derived from *vp-pow-inter-zero*

lemma (**in** *Corps*) *limit-unique*:$[\![b \in carrier\ K;\ \forall j.\ f\ j \in carrier\ K;$

valuation K v; c ∈ carrier K; lim$_{K\ v}$ *f b; lim*$_{K\ v}$ *f c*$\rrbracket \Longrightarrow$ *b = c*
⟨*proof*⟩

lemma (**in** *Corps*) *limit-n-val*:⟦*b ∈ carrier K; b ≠* **0**; *valuation K v;*
∀ j. f j ∈ carrier K; lim$_{K\ v}$ *f b*⟧ ⟹
∃ N. (∀ m. N < m ⟶ (n-val K v) (f m) = (n-val K v) b)
⟨*proof*⟩

lemma (**in** *Corps*) *limit-val*:⟦*b ∈ carrier K; b ≠* **0**; *∀ j. f j ∈ carrier K;*
valuation K v; lim$_{K\ v}$ *f b*⟧ ⟹ *∃ N. (∀ n. N < n ⟶ v (f n) = v b)*
⟨*proof*⟩

lemma (**in** *Corps*) *limit-val-infinity*:⟦*valuation K v; ∀ j. f j ∈ carrier K;*
lim$_{K\ v}$ *f* **0**⟧ ⟹ *∀ N.(∃ M. (∀ m. M < m ⟶ (an N) ≤ (n-val K v (f m))))*
⟨*proof*⟩

lemma (**in** *Corps*) *not-limit-zero*:⟦*valuation K v; ∀ j. f j ∈ carrier K;*
¬ (lim$_{K\ v}$ *f* **0**)⟧ ⟹ *∃ N.(∀ M. (∃ m. (M < m) ∧*
((n-val K v) (f m)) < (an N)))
⟨*proof*⟩

lemma (**in** *Corps*) *limit-p*:⟦*valuation K v; ∀ j. f j ∈ carrier K;*
∀ j. g j ∈ carrier K; b ∈ carrier K; c ∈ carrier K; lim$_{K\ v}$ *f b; lim*$_{K\ v}$ *g c*⟧
⟹ *lim*$_{K\ v}$ *(λj. (f j) ± (g j)) (b ± c)*
⟨*proof*⟩

lemma (**in** *Corps*) *Abs-ant-abs*[*simp*]:*Abs (ant z) = ant (abs z)*
⟨*proof*⟩

lemma (**in** *Corps*) *limit-t-nonzero*:⟦*valuation K v; ∀* (*j*::*nat*). *(f j) ∈ carrier K;*
∀ (*j*::*nat*). *g j ∈ carrier K; b ∈ carrier K; c ∈ carrier K; b ≠* **0**; *c ≠* **0**;
lim$_{K\ v}$ *f b; lim*$_{K\ v}$ *g c*⟧ ⟹ *lim*$_{K\ v}$ *(λj. (f j) ·*$_r$ *(g j)) (b ·*$_r$ *c)*
⟨*proof*⟩

lemma *an-npn*[*simp*]:*an (n + m) = an n + an m*
⟨*proof*⟩

lemma *Abs-noninf*:*a ≠ −∞ ∧ a ≠ ∞ ⟹ Abs a ≠ ∞*
⟨*proof*⟩

lemma (**in** *Corps*) *limit-t-zero*:⟦*c ∈ carrier K; valuation K v;*
∀ (*j*::*nat*). *f j ∈ carrier K; ∀* (*j*::*nat*). *g j ∈ carrier K;*
lim$_{K\ v}$ *f* **0**; *lim*$_{K\ v}$ *g c*⟧ ⟹ *lim*$_{K\ v}$ *(λj. (f j) ·*$_r$ *(g j))* **0**
⟨*proof*⟩

lemma (**in** *Corps*) *limit-minus*:⟦*valuation K v; ∀ j. f j ∈ carrier K;*
b ∈ carrier K; lim$_{K\ v}$ *f b*⟧ ⟹ *lim*$_{K\ v}$ *(λj. (−*$_a$ *(f j))) (−*$_a$ *b)*

⟨*proof*⟩

lemma (**in** *Corps*) *inv-diff*:⟦$x \in$ *carrier* K; $x \neq \mathbf{0}$; $y \in$ *carrier* K; $y \neq \mathbf{0}$⟧ ⟹
$(x^{-K}) \pm (-_a\ (y^{-K})) = (x^{-K}) \cdot_r (\ y^{-K}) \cdot_r (-_a\ (x \pm (-_a\ y)))$
⟨*proof*⟩

lemma *times2plus*:$(2::nat)*n = n + n$
⟨*proof*⟩

lemma (**in** *Corps*) *limit-inv*:⟦*valuation* K v; $\forall j.\ f\ j \in$ *carrier* K;
$b \in$ *carrier* K; $b \neq \mathbf{0}$; $lim_{K\ v}\ f\ b$⟧ ⟹
$lim_{K\ v}\ (\lambda j.\ if\ (f\ j) = \mathbf{0}\ then\ \mathbf{0}\ else\ (f\ j)^{-K})\ (b^{-K})$
⟨*proof*⟩

definition
Cauchy-seq :: [- , $'b \Rightarrow ant$, $nat \Rightarrow 'b$]
$\Rightarrow$ *bool* ((*3Cauchy* _ _ -) [*90*,*90*,*91*]*90*) **where**
$Cauchy_{K\ v}\ f \longleftrightarrow (\forall n.\ (f\ n) \in carrier\ K) \wedge (\forall N.\ \exists M.\ (\forall n\ m.\ M < n \wedge M < m \longrightarrow ((f\ n) \pm_K (-_{aK}\ (f\ m))) \in (vp\ K\ v)^{(Vr\ K\ v)\ (an\ N)}))$

definition
v-complete :: [$'b \Rightarrow ant$, -] ⇒ *bool*
((*2Complete*_ -) [*90*,*91*]*90*) **where**
$Complete_v\ K \longleftrightarrow (\forall f.\ (Cauchy_{K\ v}\ f) \longrightarrow (\exists b.\ b \in (carrier\ K) \wedge lim_{K\ v}\ f\ b))$

lemma (**in** *Corps*) *has-limit-Cauchy*:⟦*valuation* K v; $\forall j.\ f\ j \in$ *carrier* K;
$b \in$ *carrier* K; $lim_{K\ v}\ f\ b$⟧ ⟹ $Cauchy_{K\ v}\ f$
⟨*proof*⟩

lemma (**in** *Corps*) *no-limit-zero-Cauchy*:⟦*valuation* K v; $Cauchy_{K\ v}\ f$;
$\neg\ (lim_{K\ v}\ f\ \mathbf{0})$⟧ ⟹
$\exists N\ M.\ (\forall m.\ N < m \longrightarrow\ ((n\text{-}val\ K\ v)\ (f\ M))\ = ((n\text{-}val\ K\ v)\ (f\ m)))$
⟨*proof*⟩

lemma (**in** *Corps*) *no-limit-zero-Cauchy1*:⟦*valuation* K v; $\forall j.\ f\ j \in$ *carrier* K;
$Cauchy_{K\ v}\ f$; $\neg\ (lim_{K\ v}\ f\ \mathbf{0})$⟧ ⟹ $\exists N\ M.\ (\forall m.\ N < m \longrightarrow\ v\ (f\ M) = v\ (f\ m))$
⟨*proof*⟩

definition
subfield :: [-, ($'b$, $'m1$) *Ring-scheme*] ⇒ *bool* **where**
subfield $K\ K' \longleftrightarrow$ *Corps* $K' \wedge$ *carrier* $K \subseteq$ *carrier* $K' \wedge$
idmap (*carrier* K) ∈ *rHom* $K\ K'$

definition
v-completion :: [$'b \Rightarrow ant$, $'b \Rightarrow ant$, -, ($'b$, $'m$) *Ring-scheme*] ⇒ *bool*
((*4Completion*_ _ - -) [*90*,*90*,*90*,*91*]*90*) **where**
$Completion_{v\ v'}\ K\ K' \longleftrightarrow$ *subfield* $K\ K' \wedge$

$Complete_{v'}\ K' \wedge (\forall x \in carrier\ K.\ v\ x = v'\ x) \wedge$
$(\forall x \in carrier\ K'.\ (\exists f.\ Cauchy_{K\ v}\ f \wedge lim_{K'\ v'}\ f\ x))$

lemma (**in** *Corps*) *subfield-zero*:$[\![Corps\ K'; subfield\ K\ K']\!] \Longrightarrow \mathbf{0}_K = \mathbf{0}_{K'}$
⟨*proof*⟩

lemma (**in** *Corps*) *subfield-pOp*:$[\![Corps\ K'; subfield\ K\ K'; x \in carrier\ K;$
$y \in carrier\ K]\!] \Longrightarrow x \pm y = x \pm_{K'} y$
⟨*proof*⟩

lemma (**in** *Corps*) *subfield-mOp*:$[\![Corps\ K'; subfield\ K\ K'; x \in carrier\ K]\!] \Longrightarrow$
$-_a\ x = -_{a\,K'}\ x$
⟨*proof*⟩

lemma (**in** *Corps*) *completion-val-eq*:$[\![Corps\ K'; valuation\ K\ v; valuation\ K'\ v';$
$x \in carrier\ K;\ \ Completion_{v\ v'}\ K\ K']\!] \Longrightarrow v\ x = v'\ x$
⟨*proof*⟩

lemma (**in** *Corps*) *completion-subset*:$[\![Corps\ K'; valuation\ K\ v; valuation\ K'\ v';$
$Completion_{v\ v'}\ K\ K']\!] \Longrightarrow\ \ carrier\ K \subseteq carrier\ K'$
⟨*proof*⟩

lemma (**in** *Corps*) *completion-subfield*:$[\![Corps\ K'; valuation\ K\ v;$
$valuation\ K'\ v'; Completion_{v\ v'}\ K\ K']\!] \Longrightarrow\ \ subfield\ K\ K'$
⟨*proof*⟩

lemma (**in** *Corps*) *subfield-sub*:*subfield K K'* $\Longrightarrow$ *carrier K* $\subseteq$ *carrier K'*
⟨*proof*⟩

lemma (**in** *Corps*) *completion-Vring-sub*:$[\![Corps\ K'; valuation\ K\ v;$
$valuation\ K'\ v'; Completion_{v\ v'}\ K\ K']\!] \Longrightarrow$
$carrier\ (Vr\ K\ v) \subseteq carrier\ (Vr\ K'\ v')$
⟨*proof*⟩

lemma (**in** *Corps*) *completion-idmap-rHom*:$[\![Corps\ K'; valuation\ K\ v;$
$valuation\ K'\ v';\ \ Completion_{v\ v'}\ K\ K']\!] \Longrightarrow$
$I_{(Vr\ K\ v)} \in rHom\ (Vr\ K\ v)\ (Vr\ K'\ v')$
⟨*proof*⟩

lemma (**in** *Corps*) *completion-vpr-sub*:$[\![Corps\ K'; valuation\ K\ v; valuation\ K'\ v';$
$Completion_{v\ v'}\ K\ K']\!] \Longrightarrow vp\ K\ v \subseteq vp\ K'\ v'$
⟨*proof*⟩

lemma (**in** *Corps*) *val-v-completion*:$[\![Corps\ K'; valuation\ K\ v; valuation\ K'\ v';$
$x \in carrier\ K'; x \neq \mathbf{0}_{K'}; Completion_{v\ v'}\ K\ K']\!] \Longrightarrow$
$\exists f.\ (Cauchy_{K\ v}\ f) \wedge (\exists N.\ (\forall m.\ N < m \longrightarrow v\ (f\ m) = v'\ x))$
⟨*proof*⟩

lemma (**in** *Corps*) *v-completion-v-limit*:$[\![Corps\ K'; valuation\ K\ v;$

$x \in carrier\ K$; $subfield\ K\ K'$; $Complete_{v'}\ K'$; $\forall j.\ f\ j \in carrier\ K$;
$valuation\ K'\ v'$; $\forall x{\in}carrier\ K.\ v\ x = v'\ x$; $lim_{K'\ v'}\ f\ x$⟧ $\Longrightarrow$ $lim_{K\ v}\ f\ x$
⟨*proof*⟩

lemma (**in** *Corps*) *Vr-idmap-aHom*:⟦$Corps\ K'$; $valuation\ K\ v$; $valuation\ K'\ v'$;
$subfield\ K\ K'$; $\forall x{\in}carrier\ K.\ v\ x = v'\ x$⟧ $\Longrightarrow$
$I_{(Vr\ K\ v)} \in aHom\ (Vr\ K\ v)\ (Vr\ K'\ v')$
⟨*proof*⟩

lemma *amult-pos-pos*:$0 \leq a \Longrightarrow 0 \leq a * an\ N$
⟨*proof*⟩

lemma (**in** *Corps*) *Cauchy-down*:⟦$Corps\ K'$; $valuation\ K\ v$; $valuation\ K'\ v'$;
$subfield\ K\ K'$; $\forall x{\in}carrier\ K.\ v\ x = v'\ x$; $\forall j.\ f\ j \in carrier\ K$; $Cauchy_{K'\ v'}\ f$⟧
$\Longrightarrow$ $Cauchy_{K\ v}\ f$
⟨*proof*⟩

lemma (**in** *Corps*) *Cauchy-up*:⟦$Corps\ K'$; $valuation\ K\ v$; $valuation\ K'\ v'$;
$Completion_{v\ v'}\ K\ K'$; $Cauchy_{K\ v}\ f$⟧ $\Longrightarrow$ $Cauchy_{K'\ v'}\ f$
⟨*proof*⟩

lemma *max-gtTr*:$(n{::}nat) < max\ (Suc\ n)\ (Suc\ m) \wedge m < max\ (Suc\ n)\ (Suc\ m)$
⟨*proof*⟩

lemma (**in** *Corps*) *completion-approx*:⟦$Corps\ K'$; $valuation\ K\ v$; $valuation\ K'\ v'$;
$Completion_{v\ v'}\ K\ K'$; $x \in carrier\ (Vr\ K'\ v')$⟧ $\Longrightarrow$
$\exists y{\in}carrier\ (Vr\ K\ v).\ (y \pm_{K'} -_{a K'}\ x) \in (vp\ K'\ v')$

⟨*proof*⟩

lemma (**in** *Corps*) *res-v-completion-surj*:⟦ $Corps\ K'$; $valuation\ K\ v$;
$valuation\ K'\ v'$; $Completion_{v\ v'}\ K\ K'$⟧ $\Longrightarrow$
$surjec_{(Vr\ K\ v),(qring\ (Vr\ K'\ v')\ (vp\ K'\ v'))}$
$(compos\ (Vr\ K\ v)\ (pj\ (Vr\ K'\ v')\ (vp\ K'\ v'))\ (I_{(Vr\ K\ v)}))$
⟨*proof*⟩

lemma (**in** *Corps*) *res-v-completion-ker*:⟦$Corps\ K'$; $valuation\ K\ v$;
$valuation\ K'\ v'$; $Completion_{v\ v'}\ K\ K'$⟧ $\Longrightarrow$
$ker_{(Vr\ K\ v),\ (qring\ (Vr\ K'\ v')\ (vp\ K'\ v'))}$
$(compos\ (Vr\ K\ v)\ (pj\ (Vr\ K'\ v')\ (vp\ K'\ v'))\ (I_{(Vr\ K\ v)})) = vp\ K\ v$
⟨*proof*⟩

lemma (**in** *Corps*) *completion-res-qring-isom*:⟦$Corps\ K'$; $valuation\ K\ v$;
$valuation\ K'\ v'$; $Completion_{v\ v'}\ K\ K'$⟧ $\Longrightarrow$
$r\text{-}isom\ ((Vr\ K\ v)\ /_r\ (vp\ K\ v))\ ((Vr\ K'\ v')\ /_r\ (vp\ K'\ v'))$
⟨*proof*⟩

expansion of x in a complete field K, with normal valuation v. Here we suppose t is an element of K satisfying the equation $v\ t = 1$.

definition
Kxa :: [-, *'b* ⇒ *ant*, *'b*] ⇒ *'b set* **where**
Kxa K v x = {*y*. ∃*k*∈*carrier* (*Vr K v*). *y* = *x* ·$_{r\,K}$ *k*}

primrec
partial-sum :: [(*'b*, *'m*) *Ring-scheme*, *'b*, *'b* ⇒ *ant*, *'b*]
⇒ *nat* ⇒ *'b*
((*5psum* _ _ _ _ -) [*96*,*96*,*96*,*96*,*97*]*96*)
where
psum-0: *psum* $_{K\ x\ v\ t}$ *0* = (*csrp-fn* (*Vr K v*) (*vp K v*)
(*pj* (*Vr K v*) (*vp K v*) (*x* ·$_{r\,K}$ $t_K^{-(tna\ (v\ x))}$))) ·$_{r\,K}$ ($t_K^{(tna\ (v\ x))}$)
| *psum-Suc*: *psum* $_{K\ x\ v\ t}$ (*Suc n*) = (*psum* $_{K\ x\ v\ t}$ *n*) ±$_K$
((*csrp-fn* (*Vr K v*) (*vp K v*) (*pj* (*Vr K v*) (*vp K v*)
((*x* ±$_K$ −$_{a\,K}$ (*psum* $_{K\ x\ v\ t}$ *n*)) ·$_{r\,K}$ ($t_K^{-\ (tna\ (v\ x)\ +\ int\ (Suc\ n))}$)))) ·$_{r\,K}$
($t_K^{(tna\ (v\ x)\ +\ int\ (Suc\ n))}$))

definition
expand-coeff :: [- , *'b* ⇒ *ant*, *'b*, *'b*]
⇒ *nat* ⇒ *'b*
((*5ecf*_ _ _ _ -) [*96*,*96*,*96*,*96*,*97*]*96*) **where**
ecf$_{K\ v\ t\ x}$ *n* = (*if n* = *0 then csrp-fn* (*Vr K v*) (*vp K v*)
(*pj* (*Vr K v*) (*vp K v*) (*x* ·$_{r\,K}$ $t_K^{(-(tna\ (v\ x)))}$))
else csrp-fn (*Vr K v*) (*vp K v*) (*pj* (*Vr K v*)
(*vp K v*) ((*x* ±$_K$ −$_{a\,K}$ (*psum* $_{K\ x\ v\ t}$ (*n* − *1*))) ·$_{r\,K}$ ($t_K^{(-\ (tna\ (v\ x)\ +\ int\ n))}$))))

definition
expand-term :: [-, *'b* ⇒ *ant*, *'b*, *'b*]
⇒ *nat* ⇒ *'b*
((*5etm* _ _ _ _ -) [*96*,*96*,*96*,*96*,*97*]*96*) **where**

etm$_{K\ v\ t\ x}$ *n* = (*ecf*$_{K\ v\ t\ x}$ *n*)·$_{r\,K}$ ($t_K^{(tna\ (v\ x)\ +\ int\ n)}$)

lemma (**in** *Corps*) *Kxa-val-ge*:⟦*valuation K v*; *t* ∈ *carrier K*; *v t* = *1*⟧
⟹ *Kxa K v* ($t_K^{\,j}$) = {*x*. *x* ∈ *carrier K* ∧ (*ant j*) ≤ (*v x*)}
⟨*proof*⟩

lemma (**in** *Corps*) *Kxa-pow-vpr*:⟦ *valuation K v*; *t* ∈ *carrier K*; *v t* = *1*;
(*0*::*int*) ≤ *j*⟧ ⟹ *Kxa K v* ($t_K^{\,j}$) = (*vp K v*)$^{(Vr\ K\ v)\ (ant\ j)}$
⟨*proof*⟩

lemma (**in** *Corps*) *field-distribTr*:⟦*a* ∈ *carrier K*; *b* ∈ *carrier K*;
x ∈ *carrier K*; *x* ≠ **0**⟧ ⟹ *a* ± (−$_a$ (*b* ·$_r$ *x*)) = (*a* ·$_r$ (x^{-K}) ± (−$_a$ *b*)) ·$_r$ *x*

⟨*proof*⟩

lemma *a0-le-1*[*simp*]:(*0*::*ant*) ≤ *1*
⟨*proof*⟩

lemma (**in** *Corps*) *vp-mem-times-t*:⟦*valuation K v*; *t* ∈ *carrier K*; *t* ≠ **0**;
v t = *1*; *x* ∈ *vp K v*⟧ ⟹ ∃ *a*∈*carrier* (*Vr K v*). *x* = *a* ·$_r$ *t*
⟨*proof*⟩

lemma (**in** *Corps*) *psum-diff-mem-Kxa*:⟦*valuation K v*; *t* ∈ *carrier K*;
v t = *1*; *x* ∈ *carrier K*; *x* ≠ **0**⟧ ⟹
(*psum* $_{K\ x\ v\ t}$ *n*) ∈ *carrier K* ∧
(*x* ± (−$_a$ (*psum* $_{K\ x\ v\ t}$ *n*))) ∈ *Kxa K v* ($t_K^{((tna\ (v\ x))\ +\ (1\ +\ int\ n))}$)
⟨*proof*⟩

lemma *Suc-diff-int*:*0* < *n* ⟹ *int* (*n* − *Suc 0*) = *int n* − *1*
⟨*proof*⟩

lemma (**in** *Corps*) *ecf-mem*:⟦*valuation K v*; *t* ∈ *carrier K*; *v t* = *1*;
x ∈ *carrier K*; *x* ≠ **0** ⟧ ⟹ *ecf*$_{K\ v\ t\ x}$ *n* ∈ *carrier K*
⟨*proof*⟩

lemma (**in** *Corps*) *etm-mem*:⟦*valuation K v*; *t* ∈ *carrier K*; *v t* = *1*;
x ∈ *carrier K*; *x* ≠ **0**⟧ ⟹ *etm*$_{K\ v\ t\ x}$ *n* ∈ *carrier K*
⟨*proof*⟩

lemma (**in** *Corps*) *psum-sum-etm*:⟦*valuation K v*; *t* ∈ *carrier K*; *v t* = *1*;
x ∈ *carrier K*; *x* ≠ **0**⟧ ⟹
psum$_{K\ x\ v\ t}$ *n* = *nsum K* (λ*j*. (*ecf*$_{K\ v\ t\ x}$ *j*)·$_r$ ($t_K^{(tna\ (v\ x)\ +\ (int\ j))}$)) *n*
⟨*proof*⟩

lemma *zabs-pos*:*0* ≤ (*abs* (*z*::*int*))
⟨*proof*⟩

lemma *abs-p-self-pos*:*0* ≤ *z* + (*abs* (*z*::*int*))
⟨*proof*⟩

lemma *zadd-right-mono*:(*i*::*int*) ≤ *j* ⟹ *i* + *k* ≤ *j* + *k*
⟨*proof*⟩

theorem (**in** *Corps*) *expansion-thm*:⟦*valuation K v*; *t* ∈ *carrier K*;
v t = *1*; *x* ∈ *carrier K*; *x* ≠ **0**⟧ ⟹ *lim*$_{K\ v}$ (*partial-sum K x v t*) *x*
⟨*proof*⟩

2.9.1 Hensel's theorem

definition

pol-Cauchy-seq :: [('*b*, '*m*) *Ring-scheme*, '*b*, -, '*b* ⇒ *ant*,

$nat \Rightarrow 'b] \Rightarrow bool$ ((*5PCauchy* _ _ _ _ -) [*90*,*90*,*90*,*90*,*91*]*90*) **where**
PCauchy$_{R\ X\ K\ v}$ $F \longleftrightarrow (\forall\, n.\ (F\ n) \in carrier\ R) \wedge$
$(\exists\, d.\ (\forall\, n.\ deg\ R\ (Vr\ K\ v)\ X\ (F\ n) \leq (an\ d))) \wedge$
$(\forall\, N.\ \exists\, M.\ (\forall\, n\ m.\ M < n \wedge M < m \longrightarrow$
P-mod $R\ (Vr\ K\ v)\ X\ ((vp\ K\ v)^{(Vr\ K\ v)\ (an\ N)})\ (F\ n \pm_R -_a R\ (F\ m))))$

definition
pol-limit :: [('*b*, '*m*) *Ring-scheme*, '*b*, -, '*b* ⇒ *ant*,
nat ⇒ '*b*, '*b*] ⇒ *bool*
((*6Plimit* _ _ _ _ _ -) [*90*,*90*,*90*,*90*,*90*,*91*]*90*) **where**
Plimit$_{R\ X\ K\ v}$ $F\ p \longleftrightarrow (\forall\, n.\ (F\ n) \in carrier\ R) \wedge$
$(\forall\, N.\ \exists\, M.\ (\forall\, m.\ M < m \longrightarrow$
P-mod $R\ (Vr\ K\ v)\ X\ ((vp\ K\ v)^{(Vr\ K\ v)\ (an\ N)})\ ((F\ m) \pm_R -_a R\ p)))$

definition
Pseql :: [('*b*, '*m*) *Ring-scheme*, '*b*, -, '*b* ⇒ *ant*, *nat*,
nat ⇒ '*b*] ⇒ *nat* ⇒ '*b*
((*6Pseql*_ _ _ _ _ -) [*90*,*90*,*90*,*90*,*90*,*91*]*90*) **where**
Pseql$_{R\ X\ K\ v\ d}$ $F = (\lambda n.\ (ldeg\text{-}p\ R\ (Vr\ K\ v)\ X\ d\ (F\ n)))$

definition
Pseqh :: [('*b*, '*m*) *Ring-scheme*, '*b*, -, '*b* ⇒ *ant*, *nat*, *nat* ⇒ '*b*] ⇒
nat ⇒ '*b*
((*6Pseqh* _ _ _ _ _ -) [*90*,*90*,*90*,*90*,*90*,*91*]*90*) **where**
Pseqh$_{R\ X\ K\ v\ d}$ $F = (\lambda n.\ (hdeg\text{-}p\ R\ (Vr\ K\ v)\ X\ (Suc\ d)\ (F\ n)))$

lemma *an-neq-minf*[*simp*]:$\forall\, n.\ -\infty \neq an\ n$
⟨*proof*⟩

lemma *an-neq-minf1*[*simp*]:$\forall\, n.\ an\ n \neq -\infty$
⟨*proof*⟩

lemma (**in** *Corps*) *Pseql-mem*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*;
$F\ n \in carrier\ R$; $\forall\, n.\ deg\ R\ (Vr\ K\ v)\ X\ (F\ n) \leq an\ (Suc\ d)$⟧ ⟹
(*Pseql*$_{R\ X\ K\ v\ d}$ F) $n \in carrier\ R$
⟨*proof*⟩

lemma (**in** *Corps*) *Pseqh-mem*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*;
$F\ n \in carrier\ R$; $\forall\, n.\ deg\ R\ (Vr\ K\ v)\ X\ (F\ n) \leq an\ (Suc\ d)$⟧ ⟹
(*Pseqh*$_{R\ X\ K\ v\ d}$ F) $n \in carrier\ R$
⟨*proof*⟩

lemma (**in** *Corps*) *PCauchy-lTr*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*;
$p \in carrier\ R$; $deg\ R\ (Vr\ K\ v)\ X\ p \leq an\ (Suc\ d)$;
P-mod $R\ (Vr\ K\ v)\ X\ (vp\ K\ v^{(Vr\ K\ v)\ (an\ N)})\ p$⟧ ⟹

P-mod R (Vr K v) X (vp K v$^{(Vr\ K\ v)\ (an\ N)}$) (ldeg-p R (Vr K v) X d p)
⟨*proof*⟩

lemma (**in** *Corps*) *PCauchy-hTr*:⟦*valuation K v*; *PolynRg R (Vr K v) X*;
p ∈ carrier R; *deg R (Vr K v) X p ≤ an (Suc d)*;
P-mod R (Vr K v) X (vp K v$^{(Vr\ K\ v)\ (an\ N)}$) p⟧
⟹ *P-mod R (Vr K v) X (vp K v$^{(Vr\ K\ v)\ (an\ N)}$) (hdeg-p R (Vr K v) X (Suc d) p)*
⟨*proof*⟩

lemma (**in** *Corps*) *v-ldeg-p-pOp*:⟦*valuation K v*; *PolynRg R (Vr K v) X*;
p ∈ carrier R; *q ∈ carrier R*; *deg R (Vr K v) X p ≤ an (Suc d)*;
deg R (Vr K v) X q ≤ an (Suc d)⟧ ⟹
(ldeg-p R (Vr K v) X d p) ±$_R$ (ldeg-p R (Vr K v) X d q) =
ldeg-p R (Vr K v) X d (p ±$_R$ q)
⟨*proof*⟩

lemma (**in** *Corps*) *v-hdeg-p-pOp*:⟦*valuation K v*; *PolynRg R (Vr K v) X*;
p ∈ carrier R; *q ∈ carrier R*; *deg R (Vr K v) X p ≤ an (Suc d)*;
deg R (Vr K v) X q ≤ an (Suc d)⟧ ⟹ *(hdeg-p R (Vr K v) X (Suc d) p) ±$_R$*
(hdeg-p R (Vr K v) X (Suc d) q) = hdeg-p R (Vr K v) X (Suc d) (p ±$_R$ q)
⟨*proof*⟩

lemma (**in** *Corps*) *v-ldeg-p-mOp*:⟦*valuation K v*; *PolynRg R (Vr K v) X*;
p ∈ carrier R;*deg R (Vr K v) X p ≤ an (Suc d)*⟧ ⟹
−$_{aR}$ (ldeg-p R (Vr K v) X d p) = ldeg-p R (Vr K v) X d (−$_{aR}$ p)
⟨*proof*⟩

lemma (**in** *Corps*) *v-hdeg-p-mOp*:⟦*valuation K v*; *PolynRg R (Vr K v) X*;
p ∈ carrier R;*deg R (Vr K v) X p ≤ an (Suc d)*⟧ ⟹
−$_{aR}$ (hdeg-p R (Vr K v) X (Suc d) p) = hdeg-p R (Vr K v) X (Suc d) (−$_{aR}$ p)
⟨*proof*⟩

lemma (**in** *Corps*) *PCauchy-lPCauchy*:⟦*valuation K v*; *PolynRg R (Vr K v) X*;
∀ n. F n ∈ carrier R; *∀ n. deg R (Vr K v) X (F n) ≤ an (Suc d)*;
P-mod R (Vr K v) X (vp K v$^{(Vr\ K\ v)\ (an\ N)}$) (F n ±$_R$ −$_{aR}$ (F m))⟧
⟹ *P-mod R (Vr K v) X (vp K v$^{(Vr\ K\ v)\ (an\ N)}$)*
(((Pseql$_{R\ X\ K\ v\ d}$ F) n) ±$_R$ −$_{aR}$ ((Pseql$_{R\ X\ K\ v\ d}$ F) m))
⟨*proof*⟩

lemma (**in** *Corps*) *PCauchy-hPCauchy*:⟦*valuation K v*; *PolynRg R (Vr K v) X*;
∀ n. F n ∈ carrier R; *∀ n. deg R (Vr K v) X (F n) ≤ an (Suc d)*;
P-mod R (Vr K v) X (vp K v$^{(Vr\ K\ v)\ (an\ N)}$) (F n ±$_R$ −$_{aR}$ (F m))⟧
⟹ *P-mod R (Vr K v) X (vp K v$^{(Vr\ K\ v)\ (an\ N)}$)*
(((Pseqh$_{R\ X\ K\ v\ d}$ F) n) ±$_R$ −$_{aR}$ ((Pseqh$_{R\ X\ K\ v\ d}$ F) m))
⟨*proof*⟩

lemma (**in** *Corps*) *Pseq-decompos*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*;
F n ∈ *carrier R*; *deg R* (*Vr K v*) *X* (*F n*) ≤ *an* (*Suc d*)⟧
⟹ *F n* = ((*Pseql*$_{R\ X\ K\ v\ d}$ *F*) *n*) ±$_R$ ((*Pseqh*$_{R\ X\ K\ v\ d}$ *F*) *n*)
⟨*proof*⟩

lemma (**in** *Corps*) *deg-0-const*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*;
p ∈ *carrier R*; *deg R* (*Vr K v*) *X p* ≤ *0*⟧ ⟹ *p* ∈ *carrier* (*Vr K v*)
⟨*proof*⟩

lemma (**in** *Corps*) *monomial-P-limt*:⟦*valuation K v*; *Complete*$_v$ *K*;
PolynRg R (*Vr K v*) *X*; ∀ *n*. *f n* ∈ *carrier* (*Vr K v*);
∀ *n*. *F n* = (*f n*) ·$_{r\,R}$ (*X*^$\frown^R$ *d*); ∀ *N*. ∃ *M*. ∀ *n m*. *M* < *n* ∧ *M* < *m* ⟶
P-mod R (*Vr K v*) *X* (*vp K v*$^{(Vr\ K\ v)}$ (*an N*)) (*F n* ±$_R$ −$_{a\,R}$ (*F m*))⟧ ⟹
∃ *b*∈*carrier* (*Vr K v*). *Plimit* $_{R\ X\ K\ v}$ *F* (*b* ·$_{r\,R}$ (*X*^$\frown^R$ *d*))
⟨*proof*⟩

lemma (**in** *Corps*) *mPlimit-uniqueTr*:⟦*valuation K v*;
PolynRg R (*Vr K v*) *X*; ∀ *n*. *f n* ∈ *carrier* (*Vr K v*);
∀ *n*. *F n* = (*f n*) ·$_{r\,R}$ (*X*^$\frown^R$ *d*); *c* ∈ *carrier* (*Vr K v*);
Plimit $_{R\ X\ K\ v}$ *F* (*c* ·$_{r\,R}$ (*X*^$\frown^R$ *d*))⟧ ⟹ *lim* $_{K\ v}$ *f c*
⟨*proof*⟩

lemma (**in** *Corps*) *mono-P-limt-unique*:⟦*valuation K v*;
PolynRg R (*Vr K v*) *X*; ∀ *n*. *f n* ∈ *carrier* (*Vr K v*);
∀ *n*. *F n* = (*f n*) ·$_{r\,R}$ (*X*^$\frown^R$ *d*); *b* ∈ *carrier* (*Vr K v*); *c* ∈ *carrier* (*Vr K v*);
Plimit $_{R\ X\ K\ v}$ *F* (*b* ·$_{r\,R}$ (*X*^$\frown^R$ *d*)); *Plimit* $_{R\ X\ K\ v}$ *F* (*c* ·$_{r\,R}$ (*X*^$\frown^R$ *d*))⟧ ⟹
b ·$_{r\,R}$ (*X*^$\frown^R$ *d*) = *c* ·$_{r\,R}$ (*X*^$\frown^R$ *d*)
⟨*proof*⟩

lemma (**in** *Corps*) *Plimit-deg*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*;
∀ *n*. *F n* ∈ *carrier R*; ∀ *n*. *deg R* (*Vr K v*) *X* (*F n*) ≤ (*an d*);
p ∈ *carrier R*; *Plimit* $_{R\ X\ K\ v}$ *F p*⟧ ⟹ *deg R* (*Vr K v*) *X p* ≤ (*an d*)
⟨*proof*⟩

lemma (**in** *Corps*) *Plimit-deg1*:⟦*valuation K v*; *Ring R*; *PolynRg R* (*Vr K v*) *X*;
∀ *n*. *F n* ∈ *carrier R*; ∀ *n*. *deg R* (*Vr K v*) *X* (*F n*) ≤ *ad*;
p ∈ *carrier R*; *Plimit* $_{R\ X\ K\ v}$ *F p*⟧ ⟹ *deg R* (*Vr K v*) *X p* ≤ *ad*
⟨*proof*⟩

lemma (**in** *Corps*) *Plimit-ldeg*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*;
∀ *n*. *F n* ∈ *carrier R*; *p* ∈ *carrier R*;
∀ *n*. *deg R* (*Vr K v*) *X* (*F n*) ≤ *an* (*Suc d*);
Plimit $_{R\ X\ K\ v}$ *F p*⟧ ⟹ *Plimit* $_{R\ X\ K\ v}$ (*Pseql* $_{R\ X\ K\ v\ d}$ *F*)
(*ldeg-p R* (*Vr K v*) *X d p*)
⟨*proof*⟩

lemma (**in** *Corps*) *Plimit-hdeg*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*;
$\forall n.\ F\ n \in carrier\ R$; $\forall n.\ deg\ R\ (Vr\ K\ v)\ X\ (F\ n) \leq an\ (Suc\ d)$;
$p \in carrier\ R$; $Plimit_{\ R\ X\ K\ v}\ F\ p$⟧ ⟹
$Plimit_{\ R\ X\ K\ v}\ (Pseqh_{\ R\ X\ K\ v\ d}\ F)\ (hdeg\text{-}p\ R\ (Vr\ K\ v)\ X\ (Suc\ d)\ p)$
⟨*proof*⟩

lemma (**in** *Corps*) *P-limit-uniqueTr*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*⟧ ⟹
$\forall F.\ ((\forall n.\ F\ n \in carrier\ R) \wedge (\forall n.\ deg\ R\ (Vr\ K\ v)\ X\ (F\ n) \leq (an\ d)) \longrightarrow$
$(\forall p1\ p2.\ p1 \in carrier\ R \wedge p2 \in carrier\ R \wedge Plimit_{\ R\ X\ K\ v}\ F\ p1 \wedge$
$Plimit_{\ R\ X\ K\ v}\ F\ p2 \longrightarrow p1 = p2))$
⟨*proof*⟩

lemma (**in** *Corps*) *P-limit-unique*:⟦*valuation K v*; $Complete_v\ K$;
PolynRg R (*Vr K v*) *X*; $\forall n.\ F\ n \in carrier\ R$;
$\forall n.\ deg\ R\ (Vr\ K\ v)\ X\ (F\ n) \leq (an\ d)$; $p1 \in carrier\ R$; $p2 \in carrier\ R$;
$Plimit_{\ R\ X\ K\ v}\ F\ p1$; $Plimit_{\ R\ X\ K\ v}\ F\ p2$⟧ ⟹ $p1 = p2$
⟨*proof*⟩

lemma (**in** *Corps*) *P-limitTr*:⟦*valuation K v*; $Complete_v\ K$; *PolynRg R* (*Vr K v*) *X*⟧
⟹ $\forall F.\ ((\forall n.\ F\ n \in carrier\ R) \wedge (\forall n.\ deg\ R\ (Vr\ K\ v)\ X\ (F\ n) \leq (an\ d)) \wedge$
$(\forall N.\ \exists M.\ \forall n\ m.\ M < n \wedge M < m \longrightarrow$
$P\text{-}mod\ R\ (Vr\ K\ v)\ X\ (vp\ K\ v\ ^{(Vr\ K\ v)}\ (an\ N))\ (F\ n \pm_R -_a R\ (F\ m))) \longrightarrow$
$(\exists p{\in}carrier\ R.\ Plimit_{\ R\ X\ K\ v}\ F\ p))$
⟨*proof*⟩

lemma (**in** *Corps*) *PCauchy-Plimit*:⟦*valuation K v*; $Complete_v\ K$;
PolynRg R (*Vr K v*) *X*; $PCauchy_{R\ X\ K\ v}\ F$⟧ ⟹
$\exists p{\in}carrier\ R.\ Plimit_{R\ X\ K\ v}\ F\ p$
⟨*proof*⟩

lemma (**in** *Corps*) *P-limit-mult*:⟦*valuation K v*; *PolynRg R* (*Vr K v*) *X*;
$\forall n.\ F\ n \in carrier\ R$; $\forall n.\ G\ n \in carrier\ R$; $p1 \in carrier\ R$; $p2 \in carrier\ R$;
$Plimit_{\ R\ X\ K\ v}\ F\ p1$; $Plimit_{\ R\ X\ K\ v}\ G\ p2$⟧ ⟹
$Plimit_{\ R\ X\ K\ v}\ (\lambda n.\ (F\ n) \cdot_{r R}\ (G\ n))\ (p1 \cdot_{r R}\ p2)$
⟨*proof*⟩

definition
Hfst :: [-, *'b* ⇒ *ant*, (*'b*, *'m1*) *Ring-scheme*, *'b*,*'b*, (*'b set*, *'m2*) *Ring-scheme*, *'b set*, *'b*, *'b*, *'b*, *nat*] ⇒ *'b*
((*11Hfst* - - - - - - - - - - -) [67,67,67,67,67,67,67,67,67,67,68]67) **where**
$Hfst_{K\ v\ R\ X\ t\ S\ Y\ f\ g\ h}\ m = fst\ (Hpr_{R\ (Vr\ K\ v)\ X\ t\ S\ Y\ f\ g\ h}\ m)$

definition
Hsnd :: [-, *'b* ⇒ *ant*, (*'b*, *'m1*) *Ring-scheme*, *'b*,*'b*, (*'b set*, *'m2*) *Ring-scheme*, *'b set*, *'b*, *'b*, *'b*, *nat*] ⇒ *'b*
((*11Hsnd* - - - - - - - - - - -) [67,67,67,67,67,67,67,67,67,67,68]67) **where**

$Hsnd_{K\ v\ R\ X\ t\ S\ Y\ f\ g\ h}\ m = snd\ (Hpr_{R\ (Vr\ K\ v)\ X\ t\ S\ Y\ f\ g\ h}\ m)$

lemma (**in** *Corps*) *Hensel-starter*:⟦*valuation K v*; *Complete*$_v$ *K*;
PolynRg R (*Vr K v*) *X*; *PolynRg S* ((*Vr K v*) /$_r$ (*vp K v*)) *Y*;
t ∈ *carrier* (*Vr K v*); *vp K v* = (*Vr K v*) ◇$_p$ *t*;
f ∈ *carrier R*; *f* ≠ **0**$_R$; *g'* ∈ *carrier S*; *h'* ∈ *carrier S*;
0 < *deg S* ((*Vr K v*) /$_r$ (*vp K v*)) *Y g'*;
0 < *deg S* ((*Vr K v*) /$_r$ (*vp K v*)) *Y h'*;
((*erH R* (*Vr K v*) *X S* ((*Vr K v*) /$_r$ (*vp K v*)) *Y*
(*pj* (*Vr K v*) (*vp K v*))) *f*) = *g'* ·$_{rS}$ *h'*;
rel-prime-pols S ((*Vr K v*) /$_r$ (*vp K v*)) *Y g' h'*⟧ ⟹
∃ *g h*. *g* ≠ **0**$_R$ ∧ *h* ≠ **0**$_R$ ∧ *g* ∈ *carrier R* ∧ *h* ∈ *carrier R* ∧
deg R (*Vr K v*) *X g* ≤ *deg S* ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y*
(*erH R* (*Vr K v*) *X S* ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y*
(*pj* (*Vr K v*) ((*Vr K v*) ◇$_p$ *t*)) *g*) ∧ (*deg R* (*Vr K v*) *X h* +
deg S ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y* (*erH R* (*Vr K v*) *X S*
((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y* (*pj* (*Vr K v*) ((*Vr K v*) ◇$_p$ *t*)) *g*)
≤ *deg R* (*Vr K v*) *X f*) ∧
(*erH R* (*Vr K v*) *X S* ((*Vr K v*) /$_r$ (*vp K v*)) *Y*
(*pj* (*Vr K v*) (*vp K v*))) *g* = *g'* ∧
(*erH R* (*Vr K v*) *X S* ((*Vr K v*) /$_r$ (*vp K v*)) *Y*
(*pj* (*Vr K v*) (*vp K v*))) *h* = *h'* ∧
0 < *deg S* ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y*
(*erH R* (*Vr K v*) *X S* ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y*
(*pj* (*Vr K v*) ((*Vr K v*) ◇$_p$ *t*)) *g*) ∧
0 < *deg S* ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y*
(*erH R* (*Vr K v*) *X S* ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y*
(*pj* (*Vr K v*) ((*Vr K v*) ◇$_p$ *t*)) *h*) ∧
rel-prime-pols S ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y*
(*erH R* (*Vr K v*) *X S* ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y*
(*pj* (*Vr K v*) ((*Vr K v*) ◇$_p$ *t*)) *g*)
(*erH R* (*Vr K v*) *X S* ((*Vr K v*) /$_r$ ((*Vr K v*) ◇$_p$ *t*)) *Y*
(*pj* (*Vr K v*) ((*Vr K v*) ◇$_p$ *t*)) *h*) ∧
P-mod R (*Vr K v*) *X* ((*Vr K v*) ◇$_p$ *t*) (*f* ±$_R$ −$_{aR}$ (*g* ·$_{rR}$ *h*))
⟨*proof*⟩

lemma *aadd-plus-le-plus*:⟦ *a* ≤ (*a'*::*ant*); *b* ≤ *b'*⟧ ⟹ *a* + *b* ≤ *a'* + *b'*
⟨*proof*⟩

lemma (**in** *Corps*) *Hfst-PCauchy*:⟦*valuation K v*; *Complete*$_v$ *K*;
PolynRg R (*Vr K v*) *X*; *PolynRg S* (*Vr K v* /$_r$ (*Vr K v* ◇$_p$ *t*)) *Y*; *g0* ∈ *carrier R*;
h0 ∈ *carrier R*; *f* ∈ *carrier R*; *f* ≠ **0**$_R$; *g0* ≠ **0**$_R$; *h0* ≠ **0**$_R$;
t ∈ *carrier* (*Vr K v*); *vp K v* = *Vr K v* ◇$_p$ *t*;
deg R (*Vr K v*) *X g0* ≤ *deg S* (*Vr K v* /$_r$ (*Vr K v* ◇$_p$ *t*)) *Y* (*erH R* (*Vr K v*) *X S*
(*Vr K v* /$_r$ (*Vr K v* ◇$_p$ *t*)) *Y* (*pj* (*Vr K v*) (*Vr K v* ◇$_p$ *t*)) *g0*);
deg R (*Vr K v*) *X h0* + *deg S* (*Vr K v* /$_r$ (*Vr K v* ◇$_p$ *t*)) *Y* (*erH R* (*Vr K v*) *X S*
(*Vr K v* /$_r$ (*Vr K v* ◇$_p$ *t*)) *Y* (*pj* (*Vr K v*) (*Vr K v* ◇$_p$ *t*)) *g0*)
≤ *deg R* (*Vr K v*) *X f*;

$0 < deg\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (erH\ R\ (Vr\ K\ v)\ X\ S$
$(Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ g0);$
$0 < deg\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (erH\ R\ (Vr\ K\ v)\ X\ S$
$(Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ h0);$
$rel\text{-}prime\text{-}pols\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (erH\ R\ (Vr\ K\ v)\ X\ S$
$(Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ g0)$
$(erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y$
$(pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ h0);$

$erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y$
$(pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ f =$
$erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y$
$(pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ g0\ \cdot_{r S}$
$erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y$
$(pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ h0]\!] \Longrightarrow$
$PCauchy_{\ R\ X\ K\ v}\ Hfst\ K\ v\ R\ X\ t\ S\ Y\ f\ g0\ h0$

⟨*proof*⟩

lemma (**in** *Corps*) *Hsnd-PCauchy*:[![*valuation K v*; $Complete_v\ K$;
PolynRg R (*Vr K v*) *X*; *PolynRg S* (*Vr K v* $/_r$ (*Vr K v* $\diamondsuit_p$ *t*)) *Y*; *g0* ∈ *carrier R*;
h0 ∈ *carrier R*; *f* ∈ *carrier R*; $f \neq \mathbf{0}_R$; $g0 \neq \mathbf{0}_R$; $h0 \neq \mathbf{0}_R$;
t ∈ *carrier* (*Vr K v*); *vp K v* = *Vr K v* $\diamondsuit_p$ *t*;
deg R (*Vr K v*) *X g0* ≤ *deg S* (*Vr K v* $/_r$ (*Vr K v* $\diamondsuit_p$ *t*)) *Y* (*erH R* (*Vr K v*) *X S*
(*Vr K v* $/_r$ (*Vr K v* $\diamondsuit_p$ *t*)) *Y* (*pj* (*Vr K v*) (*Vr K v* $\diamondsuit_p$ *t*)) *g0*);
deg R (*Vr K v*) *X h0* + *deg S* (*Vr K v* $/_r$ (*Vr K v* $\diamondsuit_p$ *t*)) *Y* (*erH R* (*Vr K v*) *X S*
(*Vr K v* $/_r$ (*Vr K v* $\diamondsuit_p$ *t*)) *Y* (*pj* (*Vr K v*) (*Vr K v* $\diamondsuit_p$ *t*)) *g0*)
≤ *deg R* (*Vr K v*) *X f*;
$0 < deg\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (erH\ R\ (Vr\ K\ v)\ X\ S$
$(Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ g0);$
$0 < deg\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (erH\ R\ (Vr\ K\ v)\ X\ S$
$(Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ h0);$
$rel\text{-}prime\text{-}pols\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (erH\ R\ (Vr\ K\ v)\ X\ S$
$(Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y\ (pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ g0)$
$(erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y$
$(pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ h0);$
$erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y$
$(pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ f =$
$erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y$
$(pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ g0\ \cdot_{r S}$
$erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v\ /_r\ (Vr\ K\ v\ \diamondsuit_p\ t))\ Y$
$(pj\ (Vr\ K\ v)\ (Vr\ K\ v\ \diamondsuit_p\ t))\ h0]\!] \Longrightarrow$
$PCauchy_{\ R\ X\ K\ v}\ Hsnd\ K\ v\ R\ X\ t\ S\ Y\ f\ g0\ h0$

⟨*proof*⟩

lemma (**in** *Corps*) *H-Plimit-f*:[![*valuation K v*; $Complete_v\ K$;

$t \in carrier\ (Vr\ K\ v)$; $vp\ K\ v = Vr\ K\ v \diamondsuit_p\ t$;
$PolynRg\ R\ (Vr\ K\ v)\ X$; $PolynRg\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$;
$f \in carrier\ R$; $f \neq \mathbf{0}_R$; $g0 \in carrier\ R$; $h0 \in carrier\ R$; $g0 \neq \mathbf{0}_R$;
$h0 \neq \mathbf{0}_R$;
$0 < deg\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad (erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad\quad (pj\ (Vr\ K\ v)\ (Vr\ K\ v \diamondsuit_p\ t))\ g0)$;
$0 < deg\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad (erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad\quad (pj\ (Vr\ K\ v)\ (Vr\ K\ v \diamondsuit_p\ t))\ h0)$;
$deg\ R\ (Vr\ K\ v)\ X\ h0\ +$
$\quad deg\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad (erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad\quad (pj\ (Vr\ K\ v)\ (Vr\ K\ v \diamondsuit_p\ t))\ g0) \leq deg\ R\ (Vr\ K\ v)\ X\ f$;

$rel\text{-}prime\text{-}pols\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad (erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad\quad (pj\ (Vr\ K\ v)\ (Vr\ K\ v \diamondsuit_p\ t))\ g0)$
$\quad (erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad\quad (pj\ (Vr\ K\ v)\ (Vr\ K\ v \diamondsuit_p\ t))\ h0)$;

$erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad (pj\ (Vr\ K\ v)\ (Vr\ K\ v \diamondsuit_p\ t))\ f =$
$erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad (pj\ (Vr\ K\ v)\ (Vr\ K\ v \diamondsuit_p\ t))\ g0 \cdot_{r S}$
$\quad erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad\quad (pj\ (Vr\ K\ v)\ (Vr\ K\ v \diamondsuit_p\ t))\ h0$;

$\quad deg\ R\ (Vr\ K\ v)\ X\ g0$
$\quad \leq deg\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad\quad (erH\ R\ (Vr\ K\ v)\ X\ S\ (Vr\ K\ v /_r\ (Vr\ K\ v \diamondsuit_p\ t))\ Y$
$\quad\quad\quad (pj\ (Vr\ K\ v)\ (Vr\ K\ v \diamondsuit_p\ t))\ g0)$;

$g \in carrier\ R$; $h \in carrier\ R$;
$\quad Plimit_{\ R\ X\ K\ v}\ (Hfst\ K\ v\ R\ X\ t\ S\ Y\ f\ g0\ h0)\ g$;
$\quad Plimit_{\ R\ X\ K\ v}\ (Hsnd\ K\ v\ R\ X\ t\ S\ Y\ f\ g0\ h0)\ h$;
$\quad Plimit_{\ R\ X\ K\ v}\ (\lambda n.\ (Hfst_{\ K\ v\ R\ X\ t\ S\ Y\ f\ g0\ h0\ n}) \cdot_{r R}$
$\quad\quad\quad (Hsnd_{\ K\ v\ R\ X\ t\ S\ Y\ f\ g0\ h0\ n}))\ (g \cdot_{r R} h)[\![$
$\Longrightarrow Plimit_{\ R\ X\ K\ v}\ (\lambda n.\ (Hfst_{\ K\ v\ R\ X\ t\ S\ Y\ f\ g0\ h0\ n}) \cdot_{r R}$
$\quad\quad\quad (Hsnd_{\ K\ v\ R\ X\ t\ S\ Y\ f\ g0\ h0\ n}))\ f$

⟨*proof*⟩

theorem (**in** *Corps*) *Hensel*:[![$valuation\ K\ v$; $Complete_v\ K$;
$PolynRg\ R\ (Vr\ K\ v)\ X$; $PolynRg\ S\ ((Vr\ K\ v) /_r\ (vp\ K\ v))\ Y$;
$f \in carrier\ R$; $f \neq \mathbf{0}_R$; $g' \in carrier\ S$; $h' \in carrier\ S$;
$0 < deg\ S\ ((Vr\ K\ v) /_r\ (vp\ K\ v))\ Y\ g'$;
$0 < deg\ S\ ((Vr\ K\ v) /_r\ (vp\ K\ v))\ Y\ h'$;
$((erH\ R\ (Vr\ K\ v)\ X\ S\ ((Vr\ K\ v) /_r\ (vp\ K\ v))\ Y$
$\quad (pj\ (Vr\ K\ v)\ (vp\ K\ v)))\ f) = g' \cdot_{r S} h'$;

$$\begin{array}{l} \quad \textit{rel-prime-pols}\ S\ ((Vr\ K\ v)\ /_r\ (vp\ K\ v))\ Y\ g'\ h' \rrbracket \Longrightarrow \\ \exists\, g\ h.\ g \in \textit{carrier}\ R \wedge h \in \textit{carrier}\ R \wedge \\ \qquad \textit{deg}\ R\ (Vr\ K\ v)\ X\ g \leq \textit{deg}\ S\ ((Vr\ K\ v)\ /_r\ (vp\ K\ v))\ Y\ g' \wedge \\ \qquad\qquad f = g \cdot_{r\,R} h \end{array}$$

⟨*proof*⟩

end