

Fundamental Properties of Valuation Theory and Hensel's Lemma

Hidetsune Kobayashi

September 30, 2020

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

1 Preliminaries	2
1.1 Int and ant (augmented integers)	2
1.2 nsets	5
2 Elementary properties of a valuation	8
2.1 Definition of a valuation	8
2.2 The normal valuation of v	11
2.3 Valuation ring	14
2.4 Ideals in a valuation ring	17
2.4.1 Amin lemma (in Corps)s	20
2.5 pow of v_p and n -value – convergence –	21
2.6 Equivalent valuations	23
2.7 Prime divisors	24
2.8 Approximation	25
2.8.1 Representation of an ideal I as a product of prime ideals	39
2.8.2 <i>prime-n-pd</i>	42
2.9 Completion	43
2.9.1 Hensel’s theorem	50

```
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*: $(a::nat) < b \implies int\ a < int\ b$
<proof>

lemma *zless-trans*: $\llbracket (i::int) < j; j < k \rrbracket \implies i < k$
<proof>

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

lemma *zle-less-trans*: $\llbracket (i::int) \leq j; j < k \rrbracket \implies i < k$
<proof>

lemma *zless-le-trans*: $\llbracket (i::int) < j; j \leq k \rrbracket \implies i < k$
<proof>

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

lemma *ale-shift*: $\llbracket (x::ant) \leq y; y = z \rrbracket \implies x \leq z$
<proof>

lemma *aneg-na-0[simp]*: $a < 0 \implies na\ a = 0$
<proof>

lemma *amult-an-an*: $an\ (m * n) = (an\ m) * (an\ n)$
<proof>

definition

adiv :: $[ant, ant] \Rightarrow ant$ (**infixl** *adiv* 200) **where**
 $x\ adiv\ y = ant\ ((tna\ x)\ div\ (tna\ y))$

definition

$amod :: [ant, ant] \Rightarrow ant$ (**infixl** $amod$ 200) **where**

$x \ amod \ y = ant \ ((tna \ x) \ mod \ (tna \ y))$

lemma $apos-amod-conj: 0 < ant \ b \Longrightarrow$

$$0 \leq (ant \ a) \ amod \ (ant \ b) \wedge (ant \ a) \ amod \ (ant \ b) < (ant \ b)$$

$\langle proof \rangle$

lemma $amod-adiv-equality:$

$$(ant \ a) = (a \ div \ b) \ *_a \ (ant \ b) + ant \ (a \ mod \ b)$$

$\langle proof \rangle$

lemma $asp-z-Z: z \ *_a \ ant \ x \in Z_\infty$

$\langle proof \rangle$

lemma $apos-in-aug-inf: 0 \leq a \Longrightarrow a \in Z_\infty$

$\langle proof \rangle$

lemma $amult-1-both: \llbracket 0 < (w::ant); x * w = 1 \rrbracket \Longrightarrow x = 1 \wedge w = 1$

$\langle proof \rangle$

lemma $poss-int-neq-0: 0 < (z::int) \Longrightarrow z \neq 0$

$\langle proof \rangle$

lemma $aadd-neg-negg[simp]: \llbracket a \leq (0::ant); b < 0 \rrbracket \Longrightarrow a + b < 0$

$\langle proof \rangle$

lemma $aadd-two-negg[simp]: \llbracket a < (0::ant); b < 0 \rrbracket \Longrightarrow a + b < 0$

$\langle proof \rangle$

lemma $amin-aminTr: (z::ant) \leq z' \Longrightarrow amin \ z \ w \leq amin \ z' \ w$

$\langle proof \rangle$

lemma $amin-le1: (z::ant) \leq z' \Longrightarrow (amin \ z \ w) \leq z'$

$\langle proof \rangle$

lemma $amin-le2: (z::ant) \leq z' \Longrightarrow (amin \ w \ z) \leq z'$

$\langle proof \rangle$

lemma $Amin-geTr: (\forall j \leq n. f \ j \in Z_\infty) \wedge (\forall j \leq n. z \leq (f \ j)) \longrightarrow$
 $z \leq (Amin \ n \ f)$

$\langle proof \rangle$

lemma $Amin-ge: \llbracket \forall j \leq n. f \ j \in Z_\infty; \forall j \leq n. z \leq (f \ j) \rrbracket \Longrightarrow$
 $z \leq (Amin \ n \ f)$

$\langle proof \rangle$

definition

$Abs :: ant \Rightarrow ant$ **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 $int\ nat: 0 < z \implies int\ (nat\ z) = z$
(proof)

lemma $int\ ex\ nat: 0 < z \implies \exists n. int\ n = z$
(proof)

lemma $eq\ nat\ pos\ ints:$
 $\llbracket nat\ (z::int) = nat\ (z':int); 0 \leq z; 0 \leq z' \rrbracket \implies z = z'$
(proof)

lemma $a\ p1\ gt\ [simp]: \llbracket a \neq \infty; a \neq -\infty \rrbracket \implies a < a + 1$
(proof)

lemma $gt\ na\ poss: (na\ a) < m \implies 0 < m$
(proof)

lemma $azmult\ less: \llbracket a \neq \infty; na\ a < m; 0 < x \rrbracket$
 $\implies a < int\ m *_{a}\ x$
(proof)

lemma $zmult\ gt\ one: \llbracket 2 \leq m; 0 < xa \rrbracket \implies 1 < int\ m * xa$
(proof)

lemma $zmult\ pos: \llbracket 0 < m; 0 < (a::int) \rrbracket \implies 0 < (int\ m) * a$
(proof)

lemma $ant\ int\ na: \llbracket 0 \leq a; a \neq \infty \rrbracket \implies ant\ (int\ (na\ a)) = a$
(proof)

lemma $zpos\ nat: 0 \leq (z::int) \implies \exists n. z = int\ n$
(proof)

1.2 nsets

lemma *nsetTr1*: $\llbracket j \in \text{nset } a \ b; j \neq a \rrbracket \implies j \in \text{nset } (\text{Suc } a) \ b$
 $\langle \text{proof} \rangle$

lemma *nsetTr2*: $j \in \text{nset } (\text{Suc } a) \ (\text{Suc } b) \implies j - \text{Suc } 0 \in \text{nset } a \ b$
 $\langle \text{proof} \rangle$

lemma *nsetTr3*: $\llbracket j \neq \text{Suc } (\text{Suc } 0); j - \text{Suc } 0 \in \text{nset } (\text{Suc } 0) \ (\text{Suc } n) \rrbracket$
 $\implies \text{Suc } 0 < j - \text{Suc } 0$
 $\langle \text{proof} \rangle$

lemma *Suc-leD1*: $\text{Suc } m \leq n \implies m < n$
 $\langle \text{proof} \rangle$

lemma *leI1*: $n < m \implies \neg ((m::\text{nat}) \leq n)$
 $\langle \text{proof} \rangle$

lemma *neg-zle*: $\neg (z::\text{int}) \leq z' \implies z' < z$
 $\langle \text{proof} \rangle$

lemma *nset-m-m*: $\text{nset } m \ m = \{m\}$
 $\langle \text{proof} \rangle$

lemma *nset-Tr51*: $\llbracket j \in \text{nset } (\text{Suc } 0) \ (\text{Suc } (\text{Suc } n)); j \neq \text{Suc } 0 \rrbracket$
 $\implies j - \text{Suc } 0 \in \text{nset } (\text{Suc } 0) \ (\text{Suc } n)$
 $\langle \text{proof} \rangle$

lemma *nset-Tr52*: $\llbracket j \neq \text{Suc } (\text{Suc } 0); \text{Suc } 0 \leq j - \text{Suc } 0 \rrbracket$
 $\implies \neg j - \text{Suc } 0 \leq \text{Suc } 0$
 $\langle \text{proof} \rangle$

lemma *nset-Suc*: $\text{nset } (\text{Suc } 0) \ (\text{Suc } (\text{Suc } n)) =$
 $\text{nset } (\text{Suc } 0) \ (\text{Suc } n) \cup \{\text{Suc } (\text{Suc } n)\}$
 $\langle \text{proof} \rangle$

lemma *AinequalityTr0*: $x \neq -\infty \implies \exists L. (\forall N. L < N \longrightarrow$
 $(\text{an } m) < (x + \text{an } N))$
 $\langle \text{proof} \rangle$

lemma *AinequalityTr*: $\llbracket 0 < b \wedge b \neq \infty; x \neq -\infty \rrbracket \implies \exists L. (\forall N. L < N \longrightarrow$
 $(\text{an } m) < (x + (\text{int } N) *_a b))$
 $\langle \text{proof} \rangle$

lemma *two-inequalities*: $\llbracket \forall (n::\text{nat}). x < n \longrightarrow P \ n; \forall (n::\text{nat}). y < n \longrightarrow Q \ n \rrbracket$
 $\implies \forall n. (\text{max } x \ y) < n \longrightarrow (P \ n) \wedge (Q \ n)$
 $\langle \text{proof} \rangle$

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

$(\exists L. (\forall N. L < N \longrightarrow (\forall l \leq n. (an\ m) < (x\ l) + (an\ N))))$
 $\langle proof \rangle$

lemma *multi-inequalityTr1*: $\llbracket \forall j \leq (n::nat). (x\ j) \neq -\infty \rrbracket \implies$
 $\exists L. (\forall N. L < N \longrightarrow (\forall l \leq n. (an\ m) < (x\ l) + (an\ N)))$
 $\langle proof \rangle$

lemma *gcoeff-multi-inequality*: $\llbracket \forall N. 0 < N \longrightarrow (\forall j \leq (n::nat). (x\ j) \neq -\infty \wedge$
 $0 < (b\ N\ j) \wedge (b\ N\ j) \neq \infty) \rrbracket \implies$
 $\exists L. (\forall N. L < N \longrightarrow (\forall l \leq n. (an\ m) < (x\ l) + (int\ N) *_a (b\ N\ l)))$
 $\langle proof \rangle$

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*: $\forall l \leq n. (f\ l) \leq m-max\ n\ f$
 $\langle proof \rangle$

lemma *m-max-gt*: $l \leq n \implies (f\ l) \leq m-max\ n\ f$
 $\langle proof \rangle$

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

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

lemma *eSum-single*: $\llbracket \forall j \leq n. f\ j \in Z_\infty ; j \leq n ; \forall l \in \{h. h \leq n\} - \{j\}. f\ l = 0 \rrbracket$
 $\implies ASum\ f\ n = f\ j$
 $\langle proof \rangle$

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

lemma *ASum-eq*: $\llbracket \forall j \leq n. f\ j \in Z_\infty ; \forall j \leq n. g\ j \in Z_\infty ; \forall j \leq n. f\ j = g\ j \rrbracket \implies$
 $ASum\ f\ n = ASum\ g\ n$
 $\langle proof \rangle$

definition

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

definition

$K\text{-gamma} :: [\text{nat}, \text{nat}] \Rightarrow \text{int}$
 $((\gamma _ _) [\gamma 0, \gamma 1] \gamma 0)$ **where**
 $\gamma_i j = (\text{if } i = j \text{ then } 0 \text{ else } 1)$

abbreviation

$\text{TRANSPOS } ((\tau _ _) [90, 91] 90)$ **where**
 $\tau_i j == \text{transpos } i j$

lemma $K\text{delta-in-Zinf} : \llbracket j \leq (\text{Suc } n); k \leq (\text{Suc } n) \rrbracket \Longrightarrow$
 $z *_{\text{a}} (\delta_j k) \in Z_{\infty}$
 $\langle \text{proof} \rangle$

lemma $K\text{delta-in-Zinf1} : \llbracket j \leq n; k \leq n \rrbracket \Longrightarrow \delta_j k \in Z_{\infty}$
 $\langle \text{proof} \rangle$

primrec $m\text{-zmax} :: [\text{nat}, \text{nat} \Rightarrow \text{int}] \Rightarrow \text{int}$
where

$m\text{-zmax-0} : m\text{-zmax } 0 f = f 0$
 $| m\text{-zmax-Suc} : m\text{-zmax } (\text{Suc } n) f = \text{zmax } (m\text{-zmax } n f) (f (\text{Suc } n))$

lemma $m\text{-zmax-gt-eachTr} :$
 $(\forall j \leq n. f j \in Z\text{set}) \longrightarrow (\forall j \leq n. (f j) \leq m\text{-zmax } n f)$
 $\langle \text{proof} \rangle$

lemma $m\text{-zmax-gt-each} : (\forall j \leq n. f j \in Z\text{set}) \Longrightarrow (\forall j \leq n. (f j) \leq m\text{-zmax } n f)$
 $\langle \text{proof} \rangle$

lemma $n\text{-notin-Nset-pred} : 0 < n \Longrightarrow \neg n \leq (n - \text{Suc } 0)$
 $\langle \text{proof} \rangle$

lemma $N\text{set-preTr} : \llbracket 0 < n; j \leq (n - \text{Suc } 0) \rrbracket \Longrightarrow j \leq n$
 $\langle \text{proof} \rangle$

lemma $N\text{set-preTr1} : \llbracket 0 < n; j \leq (n - \text{Suc } 0) \rrbracket \Longrightarrow j \neq n$
 $\langle \text{proof} \rangle$

lemma $\text{transpos-noteqTr} : \llbracket 0 < n; k \leq (n - \text{Suc } 0); j \leq n; j \neq n \rrbracket$
 $\Longrightarrow j \neq (\tau_j n) k$
 $\langle \text{proof} \rangle$

Chapter 2

Elementary properties of a valuation

2.1 Definition of a valuation

definition

valuation :: [(*'b*, *'m*) Ring-scheme, *'b* ⇒ *ant*] ⇒ *bool* **where**

valuation *K* *v* ⇔

$v \in \text{extensional } (\text{carrier } K) \wedge$

$v \in \text{carrier } K \rightarrow Z_\infty \wedge$

$v (\mathbf{0}_K) = \infty \wedge (\forall x \in ((\text{carrier } K) - \{\mathbf{0}_K\}). v x \neq \infty) \wedge$

$(\forall x \in (\text{carrier } K). \forall y \in (\text{carrier } K). v (x \cdot_r K y) = (v x) + (v y)) \wedge$

$(\forall x \in (\text{carrier } K). 0 \leq (v x) \rightarrow 0 \leq (v (1_r K \pm_K x))) \wedge$

$(\exists x. x \in \text{carrier } K \wedge (v x) \neq \infty \wedge (v x) \neq 0)$

lemma (in *Corps*) *invf-closed*: $x \in \text{carrier } K - \{\mathbf{0}\} \implies x^{-K} \in \text{carrier } K$

<proof>

lemma (in *Corps*) *valuation-map*: $\text{valuation } K v \implies v \in \text{carrier } K \rightarrow Z_\infty$

<proof>

lemma (in *Corps*) *value-in-aug-inf*: $[\text{valuation } K v; x \in \text{carrier } K] \implies$

$v x \in Z_\infty$

<proof>

lemma (in *Corps*) *value-of-zero*: $\text{valuation } K v \implies v (\mathbf{0}) = \infty$

<proof>

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

$\implies (v x) \neq \infty$

<proof>

lemma (in *Corps*) *value-inf-zero*: $[\text{valuation } K v; x \in \text{carrier } K; v x = \infty]$

$\implies x = \mathbf{0}$

<proof>

lemma (in *Corps*) *val-nonzero-z*: $\llbracket \text{valuation } K v; x \in \text{carrier } K; x \neq \mathbf{0} \rrbracket \implies$
 $\exists z. (v x) = \text{ant } z$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-nonzero-z-unique*: $\llbracket \text{valuation } K v; x \in \text{carrier } K; x \neq \mathbf{0} \rrbracket$
 $\implies \exists! z. (v x) = \text{ant } z$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *value-noninf-nonzero*: $\llbracket \text{valuation } K v; x \in \text{carrier } K; v x \neq \infty \rrbracket$
 $\implies x \neq \mathbf{0}$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val1-neq-0*: $\llbracket \text{valuation } K v; x \in \text{carrier } K; v x = 1 \rrbracket \implies$
 $x \neq \mathbf{0}$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-Zmin-sym*: $\llbracket \text{valuation } K v; x \in \text{carrier } K; y \in \text{carrier } K \rrbracket$
 $\implies \text{amin } (v x) (v y) = \text{amin } (v y) (v x)$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-t2p*: $\llbracket \text{valuation } K v; x \in \text{carrier } K; y \in \text{carrier } K \rrbracket$
 $\implies v (x \cdot_r y) = v x + v y$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-axiom4*: $\llbracket \text{valuation } K v; x \in \text{carrier } K; 0 \leq v x \rrbracket \implies$
 $0 \leq v (1_r \pm x)$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-axiom5*: $\text{valuation } K v \implies$
 $\exists x. x \in \text{carrier } K \wedge v x \neq \infty \wedge v x \neq 0$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-field-nonzero*: $\text{valuation } K v \implies \text{carrier } K \neq \{\mathbf{0}\}$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-field-1-neq-0*: $\text{valuation } K v \implies 1_r \neq \mathbf{0}$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *value-of-one*: $\text{valuation } K v \implies v (1_r) = 0$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *has-val-one-neq-zero*: $\text{valuation } K v \implies 1_r \neq \mathbf{0}$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-minus-one*: $\text{valuation } K v \implies v (-_a 1_r) = 0$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-minus-eq*: $\llbracket \text{valuation } K v; x \in \text{carrier } K \rrbracket \implies$

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

<proof>

lemma (in Corps) *value-of-inv*: \llbracket valuation K v ; $x \in$ carrier K ; $x \neq \mathbf{0}$ $\rrbracket \implies$
 $v (x^{-K}) = - (v x)$

<proof>

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

<proof>

exponent in a field

lemma (in Corps) *val-exp*: \llbracket valuation K v ; $x \in$ carrier K ; $x \neq \mathbf{0}$ $\rrbracket \implies$
 $z *_a (v x) = v (x_{K^z})$

<proof>

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

<proof>

lemma (in Corps) *v-ale-diff*: \llbracket valuation K v ; $x \in$ carrier K ; $y \in$ carrier K ;
 $x \neq \mathbf{0}$; $v x \leq v y$ $\rrbracket \implies 0 \leq v(y \cdot_r x^{-K})$

<proof>

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

<proof>

lemma (in Corps) *amin-le-plus*: \llbracket valuation K v ; $x \in$ carrier K ; $y \in$ carrier K \rrbracket
 $\implies (amin (v x) (v y)) \leq (v (x \pm y))$

<proof>

lemma (in Corps) *value-less-eq*: \llbracket valuation K v ; $x \in$ carrier K ; $y \in$ carrier K ;
 $(v x) < (v y)$ $\rrbracket \implies (v x) = (v (x \pm y))$

<proof>

lemma (in Corps) *value-less-eq1*: \llbracket valuation K v ; $x \in$ carrier K ; $y \in$ carrier K ;
 $(v x) < (v y)$ $\rrbracket \implies v x = v (y \pm x)$

<proof>

lemma (in Corps) *val-1px*: \llbracket valuation K v ; $x \in$ carrier K ; $0 \leq (v (1_r \pm x))$ \rrbracket
 $\implies 0 \leq (v x)$

<proof>

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

<proof>

2.2 The normal valuation of v

definition

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

definition

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

definition

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

lemma (in Corps) vals-pos-nonempty:valuation $K v \Longrightarrow$
 $\{x. x \in v \text{ ' carrier } K \wedge 0 < x\} \neq \{\}$

<proof>

lemma (in Corps) vals-pos-LBset:valuation $K v \Longrightarrow$
 $\{x. x \in v \text{ ' carrier } K \wedge 0 < x\} \subseteq \text{LBset } 1$

<proof>

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

<proof>

lemma (in Corps) AMin-z:valuation $K v \Longrightarrow$
 $\exists a. AMin \{x. x \in v \text{ ' carrier } K \wedge 0 < x\} = \text{ant } a$

<proof>

lemma (in Corps) Lv-z:valuation $K v \Longrightarrow \exists z. Lv K v = \text{ant } z$

<proof>

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

<proof>

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

<proof>

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

<proof>

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

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-principalTr2*: $\llbracket \text{valuation } K v; c \in v \text{ ' } (\text{carrier } K - \{0\}) \wedge (\forall w \in v \text{ ' } \text{carrier } K. \exists a. w = a * c) \wedge 0 < c; d \in v \text{ ' } (\text{carrier } K - \{0\}) \wedge (\forall w \in v \text{ ' } \text{carrier } K. \exists a. w = a * d) \wedge 0 < d \rrbracket \implies c = d$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *val-principal*: $\text{valuation } K v \implies \exists! x0. x0 \in v \text{ ' } (\text{carrier } K - \{0\}) \wedge (\forall w \in v \text{ ' } (\text{carrier } K). \exists (a::\text{ant}). w = a * x0) \wedge 0 < x0$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *n-val-defTr*: $\llbracket \text{valuation } K v; w \in \text{carrier } K \rrbracket \implies \exists! a. a * Lv K v = v w$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *n-valTr*: $\llbracket \text{valuation } K v; x \in \text{carrier } K \rrbracket \implies (\text{THE } l. (l * (Lv K v)) = v x) * (Lv K v) = v x$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *n-val*: $\llbracket \text{valuation } K v; x \in \text{carrier } K \rrbracket \implies (n\text{-val } K v x) * (Lv K v) = v x$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *val-pos-n-val-pos*: $\llbracket \text{valuation } K v; x \in \text{carrier } K \rrbracket \implies (0 \leq v x) = (0 \leq n\text{-val } K v x)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *n-val-in-aug-inf*: $\llbracket \text{valuation } K v; x \in \text{carrier } K \rrbracket \implies n\text{-val } K v x \in Z_\infty$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *n-val-0*: $\llbracket \text{valuation } K v; x \in \text{carrier } K; v x = 0 \rrbracket \implies n\text{-val } K v x = 0$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *value-n0-n-val-n0*: $\llbracket \text{valuation } K v; x \in \text{carrier } K; v x \neq 0 \rrbracket \implies n\text{-val } K v x \neq 0$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *val-0-n-val-0*: $\llbracket \text{valuation } K v; x \in \text{carrier } K \rrbracket \implies (v x = 0) = (n\text{-val } K v x = 0)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *val-noninf-n-val-noninf*: $\llbracket \text{valuation } K v; x \in \text{carrier } K \rrbracket \implies (v x \neq \infty) = (n\text{-val } K v x \neq \infty)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *val-inf-n-val-inf*: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K \rrbracket \implies$
 $(v \ x = \infty) = (n\text{-val } K \ v \ x = \infty)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *val-eq-n-val-eq*: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K; y \in \text{carrier } K \rrbracket \implies$
 $(v \ x = v \ y) = (n\text{-val } K \ v \ x = n\text{-val } K \ v \ y)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *val-poss-n-val-poss*: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K \rrbracket \implies$
 $(0 < v \ x) = (0 < n\text{-val } K \ v \ x)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *n-val-Pg*: $\text{valuation } K \ v \implies n\text{-val } K \ v \ (Pg \ K \ v) = 1$
 $\langle \text{proof} \rangle$

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

lemma (in *Corps*) *n-val-t2p*: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K; y \in \text{carrier } K \rrbracket \implies$
 $n\text{-val } K \ v \ (x \cdot_r \ y) = n\text{-val } K \ v \ x + (n\text{-val } K \ v \ y)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *n-val-valuationTr2*: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K; y \in \text{carrier } K \rrbracket \implies$
 $\text{amin } (n\text{-val } K \ v \ x) \ (n\text{-val } K \ v \ y) \leq (n\text{-val } K \ v \ (x \pm y))$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *n-val-valuation*: $\text{valuation } K \ v \implies$
 $\text{valuation } K \ (n\text{-val } K \ v)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *n-val-le-val*: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K; 0 \leq (v \ x) \rrbracket \implies$
 $(n\text{-val } K \ v \ x) \leq (v \ x)$
 $\langle \text{proof} \rangle$

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

lemma (in *Corps*) *n-value-in-aug-inf*: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K \rrbracket \implies$
 $n\text{-val } K \ v \ x \in Z_\infty$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *val-surj-n-valTr*: $\llbracket \text{valuation } K \ v; \exists x \in \text{carrier } K. v \ x = 1 \rrbracket \implies$
 $Lv \ K \ v = 1$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *val-surj-n-val*: $\llbracket \text{valuation } K \ v; \exists x \in \text{carrier } K. v \ x = 1 \rrbracket \implies$

$$(n\text{-val } K \ v) = v$$

<proof>

lemma (in *Corps*) *n-val-n-val:valuation* $K \ v \implies$
 $n\text{-val } K \ (n\text{-val } K \ v) = n\text{-val } K \ v$

<proof>

lemma *nnonzero-annonzero:0 < N* $\implies an \ N \neq 0$
<proof>

2.3 Valuation ring

definition

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

definition

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

definition

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

abbreviation

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

lemma (in *Ring*) *ring-pow-apow:ideal* $R \ I \implies$
 $I \diamond R \ n = I^R \ (an \ n)$

<proof>

lemma (in *Ring*) *r-apow-Suc:ideal* $R \ I \implies I^R \ (an \ (Suc \ 0)) = I$
<proof>

lemma (in *Ring*) *apow-ring-pow:ideal* $R \ I \implies$
 $I \diamond R \ n = I^R \ (an \ n)$

<proof>

lemma (in *Corps*) *Vr-ring:valuation* $K \ v \implies Ring \ (Vr \ K \ v)$
<proof>

lemma (in *Corps*) *val-pos-mem-Vr:[valuation* $K \ v; x \in carrier \ K]$ \implies
 $(0 \leq (v \ x)) = (x \in carrier \ (Vr \ K \ v))$

<proof>

lemma (in Corps) *val-poss-mem-Vr*: \llbracket valuation $K v$; $x \in \text{carrier } K$; $0 < (v x)$ \rrbracket
 $\implies x \in \text{carrier } (Vr K v)$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-one*:valuation $K v \implies 1_r K \in \text{carrier } (Vr K v)$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-mem-f-mem*: \llbracket valuation $K v$; $x \in \text{carrier } (Vr K v)$ \rrbracket
 $\implies x \in \text{carrier } K$

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-1-f-1*:valuation $K v \implies 1_r(Vr K v) = 1_r$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-pOp-f-pOp*: \llbracket valuation $K v$; $x \in \text{carrier } (Vr K v)$;
 $y \in \text{carrier } (Vr K v)$ $\rrbracket \implies x \pm_{Vr K v} y = x \pm y$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-mOp-f-mOp*: \llbracket valuation $K v$; $x \in \text{carrier } (Vr K v)$ \rrbracket
 $\implies -_a(Vr K v) x = -_a x$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-tOp-f-tOp*: \llbracket valuation $K v$; $x \in \text{carrier } (Vr K v)$;
 $y \in \text{carrier } (Vr K v)$ $\rrbracket \implies x \cdot_r(Vr K v) y = x \cdot_r y$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-pOp-le*: \llbracket valuation $K v$; $x \in \text{carrier } K$;
 $y \in \text{carrier } (Vr K v)$ $\rrbracket \implies v x \leq (v x + (v y))$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-integral*:valuation $K v \implies \text{Idomain } (Vr K v)$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-exp-mem*: \llbracket valuation $K v$; $x \in \text{carrier } (Vr K v)$ \rrbracket
 $\implies x^{K n} \in \text{carrier } (Vr K v)$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-exp-f-exp*: \llbracket valuation $K v$; $x \in \text{carrier } (Vr K v)$ $\rrbracket \implies$
 $x^{(Vr K v) n} = x^{K n}$

$\langle \text{proof} \rangle$

lemma (in Corps) *Vr-potent-nonzero*: \llbracket valuation $K v$;
 $x \in \text{carrier } (Vr K v) - \{\mathbf{0}_{Vr K v}\}$ $\rrbracket \implies x^{K n} \neq \mathbf{0}_{Vr K v}$

$\langle \text{proof} \rangle$

lemma (in Corps) *elem-0-val-if*: \llbracket valuation $K v$; $x \in \text{carrier } K$; $v x = 0$ \rrbracket
 $\implies x \in \text{carrier } (Vr K v) \wedge x^{-K} \in \text{carrier } (Vr K v)$

<proof>

lemma (in Corps) *elem0val*: \llbracket valuation $K v$; $x \in \text{carrier } K$; $x \neq \mathbf{0}$ $\rrbracket \implies$
 $(v x = 0) = (x \in \text{carrier } (Vr K v) \wedge x^{-K} \in \text{carrier } (Vr K v))$

<proof>

lemma (in Corps) *ideal-inc-elem0val-whole*: \llbracket valuation $K v$; $x \in \text{carrier } K$;
 $v x = 0$; ideal $(Vr K v) I$; $x \in I$ $\rrbracket \implies I = \text{carrier } (Vr K v)$

<proof>

lemma (in Corps) *vp-mem-Vr-mem*: \llbracket valuation $K v$; $x \in (vp K v)$ $\rrbracket \implies$
 $x \in \text{carrier } (Vr K v)$

<proof>

lemma (in Corps) *vp-mem-val-poss*: \llbracket valuation $K v$; $x \in \text{carrier } K$ $\rrbracket \implies$
 $(x \in vp K v) = (0 < (v x))$

<proof>

lemma (in Corps) *Pg-in-Vr*: $\text{valuation } K v \implies Pg K v \in \text{carrier } (Vr K v)$

<proof>

lemma (in Corps) *vp-ideal*: $\text{valuation } K v \implies \text{ideal } (Vr K v) (vp K v)$

<proof>

lemma (in Corps) *vp-not-whole*: $\text{valuation } K v \implies$
 $(vp K v) \neq \text{carrier } (Vr K v)$

<proof>

lemma (in Ring) *elem-out-ideal-nonzero*: \llbracket ideal $R I$; $x \in \text{carrier } R$;
 $x \notin I$ $\rrbracket \implies x \neq \mathbf{0}_R$

<proof>

lemma (in Corps) *vp-prime*: $\text{valuation } K v \implies \text{prime-ideal } (Vr K v) (vp K v)$

<proof>

lemma (in Corps) *vp-pow-ideal*: $\text{valuation } K v \implies$
 $\text{ideal } (Vr K v) ((vp K v) \diamond (Vr K v) n)$

<proof>

lemma (in Corps) *vp-apow-ideal*: \llbracket valuation $K v$; $0 \leq n$ $\rrbracket \implies$
 $\text{ideal } (Vr K v) ((vp K v)^{(Vr K v) n})$

<proof>

lemma (in Corps) *mem-vp-apow-mem-Vr*: \llbracket valuation $K v$;
 $0 \leq N$; $x \in vp K v (Vr K v) N$ $\rrbracket \implies x \in \text{carrier } (Vr K v)$

<proof>

lemma (in *Corps*) *elem-out-vp-unit*: \llbracket valuation $K v$; $x \in \text{carrier } (Vr K v)$;
 $x \notin vp K v \rrbracket \implies v x = 0$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *vp-maximal:valuation $K v \implies$*
maximal-ideal $(Vr K v) (vp K v)$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *ideal-sub-vp*: \llbracket valuation $K v$; ideal $(Vr K v) I$;
 $I \neq \text{carrier } (Vr K v) \rrbracket \implies I \subseteq (vp K v)$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *Vr-local*: \llbracket valuation $K v$; maximal-ideal $(Vr K v) I \rrbracket \implies$
 $(vp K v) = I$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *v-residue-field:valuation $K v \implies$*
Corps $((Vr K v) /_r (vp K v))$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *Vr-n-val-Vr:valuation $K v \implies$*
carrier $(Vr K v) = \text{carrier } (Vr K (n\text{-val } K v))$

$\langle \text{proof} \rangle$

2.4 Ideals in a valuation ring

lemma (in *Corps*) *Vr-has-poss-elem:valuation $K v \implies$*
 $\exists x \in \text{carrier } (Vr K v) - \{\mathbf{0}_{Vr K v}\}. 0 < v x$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *vp-nonzero:valuation $K v \implies vp K v \neq \{\mathbf{0}_{Vr K v}\}$*

$\langle \text{proof} \rangle$

lemma (in *Corps*) *field-frac-mul*: $\llbracket x \in \text{carrier } K$; $y \in \text{carrier } K$; $y \neq \mathbf{0} \rrbracket$
 $\implies x = (x \cdot_r (y^{-K})) \cdot_r y$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *elems-le-val*: \llbracket valuation $K v$; $x \in \text{carrier } K$; $y \in \text{carrier } K$;
 $x \neq \mathbf{0}$; $v x \leq (v y) \rrbracket \implies \exists r \in \text{carrier } (Vr K v). y = r \cdot_r x$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-Rxa-gt-a*: \llbracket valuation $K v$; $x \in \text{carrier } (Vr K v) - \{\mathbf{0}\}$;
 $y \in \text{carrier } (Vr K v)$; $y \in Rxa (Vr K v) x \rrbracket \implies v x \leq (v y)$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-Rxa-gt-a-1*: \llbracket valuation $K v$; $x \in \text{carrier } (Vr K v)$;
 $y \in \text{carrier } (Vr K v)$; $x \neq \mathbf{0}$; $v x \leq (v y) \rrbracket \implies y \in Rxa (Vr K v) x$

$\langle \text{proof} \rangle$

lemma (in Corps) *equal-inv*: \llbracket valuation K v ; $x \in \text{carrier } K$; $y \in \text{carrier } K$;
 $y \neq \mathbf{0}$; $v x = v y$ $\rrbracket \implies 0 = v (x \cdot_r (y^{-K}))$
 <proof>

lemma (in Corps) *eq-val-eq-idealTr*: \llbracket valuation K v ;
 $x \in \text{carrier } (Vr K v) - \{\mathbf{0}\}$; $y \in \text{carrier } (Vr K v)$; $v x \leq (v y)$ $\rrbracket \implies$
 $Rxa (Vr K v) y \subseteq Rxa (Vr K v) x$
 <proof>

lemma (in Corps) *eq-val-eq-ideal*: \llbracket valuation K v ;
 $x \in \text{carrier } (Vr K v)$; $y \in \text{carrier } (Vr K v)$; $v x = v y$ \rrbracket
 $\implies Rxa (Vr K v) x = Rxa (Vr K v) y$
 <proof>

lemma (in Corps) *eq-ideal-eq-val*: \llbracket valuation K v ; $x \in \text{carrier } (Vr K v)$;
 $y \in \text{carrier } (Vr K v)$; $Rxa (Vr K v) x = Rxa (Vr K v) y$ $\rrbracket \implies v x = v y$
 <proof>

lemma (in Corps) *zero-val-gen-whole*:
 \llbracket valuation K v ; $x \in \text{carrier } (Vr K v)$ $\rrbracket \implies$
 $(v x = 0) = (Rxa (Vr K v) x = \text{carrier } (Vr K v))$
 <proof>

lemma (in Corps) *elem-nonzeroval-gen-proper*: \llbracket valuation K v ;
 $x \in \text{carrier } (Vr K v)$; $v x \neq 0$ $\rrbracket \implies Rxa (Vr K v) x \neq \text{carrier } (Vr K v)$
 <proof>

We prove that $Vr K v$ is a principal ideal ring

definition

$LI :: [(r, 'm) \text{ Ring-scheme}, 'r \Rightarrow \text{ant}, 'r \text{ set}] \Rightarrow \text{ant}$ **where**

$$LI K v I = AMin (v ' I)$$

definition

$Ig :: [(r, 'm) \text{ Ring-scheme}, 'r \Rightarrow \text{ant}, 'r \text{ set}] \Rightarrow 'r$ **where**

$$Ig K v I = (\text{SOME } x. x \in I \wedge v x = LI K v I)$$

lemma (in Corps) *val-in-image*: \llbracket valuation K v ; ideal $(Vr K v) I$; $x \in I$ $\rrbracket \implies$
 $v x \in v ' I$
 <proof>

lemma (in Corps) *I-vals-nonempty*: \llbracket valuation K v ; ideal $(Vr K v) I$ $\rrbracket \implies$
 $v ' I \neq \{\}$
 <proof>

lemma (in Corps) *I-vals-LBset*: \llbracket valuation K v ; ideal $(Vr K v) I$ $\rrbracket \implies$
 $v ' I \subseteq LBset 0$
 <proof>

lemma (in Corps) *LI-pos*: $\llbracket \text{valuation } K v; \text{ideal } (Vr K v) I \rrbracket \implies 0 \leq LI K v I$
 \langle proof \rangle

lemma (in Corps) *LI-poss*: $\llbracket \text{valuation } K v; \text{ideal } (Vr K v) I; I \neq \text{carrier } (Vr K v) \rrbracket \implies 0 < LI K v I$
 \langle proof \rangle

lemma (in Corps) *LI-z*: $\llbracket \text{valuation } K v; \text{ideal } (Vr K v) I; I \neq \{\mathbf{0}_{Vr K v}\} \rrbracket \implies \exists z. LI K v I = \text{ant } z$
 \langle proof \rangle

lemma (in Corps) *LI-k*: $\llbracket \text{valuation } K v; \text{ideal } (Vr K v) I \rrbracket \implies \exists k \in I. LI K v I = v k$
 \langle proof \rangle

lemma (in Corps) *LI-infinity*: $\llbracket \text{valuation } K v; \text{ideal } (Vr K v) I \rrbracket \implies (LI K v I = \infty) = (I = \{\mathbf{0}_{Vr K v}\})$
 \langle proof \rangle

lemma (in Corps) *val-Ig*: $\llbracket \text{valuation } K v; \text{ideal } (Vr K v) I \rrbracket \implies (Ig K v I) \in I \wedge v (Ig K v I) = LI K v I$
 \langle proof \rangle

lemma (in Corps) *Ig-nonzero*: $\llbracket \text{valuation } K v; \text{ideal } (Vr K v) I; I \neq \{\mathbf{0}_{Vr K v}\} \rrbracket \implies (Ig K v I) \neq \mathbf{0}$
 \langle proof \rangle

lemma (in Corps) *Vr-ideal-npowf-closed*: $\llbracket \text{valuation } K v; \text{ideal } (Vr K v) I; x \in I; 0 < n \rrbracket \implies x_K^n \in I$
 \langle proof \rangle

lemma (in Corps) *Ig-generate-I*: $\llbracket \text{valuation } K v; \text{ideal } (Vr K v) I \rrbracket \implies (Vr K v) \diamond_p (Ig K v I) = I$
 \langle proof \rangle

lemma (in Corps) *Pg-gen-vp*: $\text{valuation } K v \implies (Vr K v) \diamond_p (Pg K v) = vp K v$
 \langle proof \rangle

lemma (in Corps) *vp-gen-t*: $\text{valuation } K v \implies \exists t \in \text{carrier } (Vr K v). vp K v = (Vr K v) \diamond_p t$
 \langle proof \rangle

lemma (in Corps) *vp-gen-nonzero*: $\llbracket \text{valuation } K v; vp K v = (Vr K v) \diamond_p t \rrbracket \implies t \neq \mathbf{0}_{Vr K v}$
 \langle proof \rangle

lemma (in Corps) *n-value-idealTr*: $\llbracket \text{valuation } K v; 0 \leq n \rrbracket \implies$

$$(vp \ K \ v) \diamond (Vr \ K \ v) \ n = Vr \ K \ v \diamond_p ((Pg \ K \ v) \wedge (Vr \ K \ v) \ n)$$

<proof>

lemma (in *Corps*) *ideal-pow-vp*: $\llbracket valuation \ K \ v; ideal \ (Vr \ K \ v) \ I; I \neq carrier \ (Vr \ K \ v); I \neq \{\mathbf{0}_{Vr \ K \ v}\} \rrbracket \implies$
 $I = (vp \ K \ v) \diamond (Vr \ K \ v) \ (na \ (n-val \ K \ v \ (Ig \ K \ v \ I)))$

<proof>

lemma (in *Corps*) *ideal-apow-vp*: $\llbracket valuation \ K \ v; ideal \ (Vr \ K \ v) \ I \rrbracket \implies$
 $I = (vp \ K \ v) \ (Vr \ K \ v) \ (n-val \ K \ v \ (Ig \ K \ v \ I))$

<proof>

lemma (in *Corps*) *ideal-apow-n-val*: $\llbracket valuation \ K \ v; x \in carrier \ (Vr \ K \ v) \rrbracket \implies$
 $(Vr \ K \ v) \diamond_p \ x = (vp \ K \ v) \ (Vr \ K \ v) \ (n-val \ K \ v \ x)$

<proof>

lemma (in *Corps*) *t-gen-vp*: $\llbracket valuation \ K \ v; t \in carrier \ K; v \ t = 1 \rrbracket \implies$
 $(Vr \ K \ v) \diamond_p \ t = vp \ K \ v$

<proof>

lemma (in *Corps*) *t-vp-apow*: $\llbracket valuation \ K \ v; t \in carrier \ K; v \ t = 1 \rrbracket \implies$
 $(Vr \ K \ v) \diamond_p \ (t \wedge (Vr \ K \ v) \ n) = (vp \ K \ v) \ (Vr \ K \ v) \ (an \ n)$

<proof>

<proof>

lemma (in *Corps*) *nonzeroelem-gen-nonzero*: $\llbracket valuation \ K \ v; x \neq \mathbf{0}; x \in carrier \ (Vr \ K \ v) \rrbracket \implies Vr \ K \ v \diamond_p \ x \neq \{\mathbf{0}_{Vr \ K \ v}\}$

<proof>

2.4.1 Amin lemma (in Corps)s

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

<proof>

lemma (in *Corps*) *Amin-le-add*: $\llbracket valuation \ K \ v; \forall j \leq n. f \ j \in carrier \ K \rrbracket \implies$
 $Amin \ n \ (v \circ f) \leq (v \ (nsum \ K \ f \ n))$

<proof>

lemma (in *Corps*) *value-ge-add*: $\llbracket valuation \ K \ v; \forall j \leq n. f \ j \in carrier \ K; \forall j \leq n. z \leq ((v \circ f) \ j) \rrbracket \implies z \leq (v \ (\Sigma_e \ K \ f \ n))$

<proof>

lemma (in *Corps*) *Vr-ideal-powTr1*: $\llbracket valuation \ K \ v; ideal \ (Vr \ K \ v) \ I; \rrbracket$

$I \neq \text{carrier } (Vr K v); b \in I \implies b \in (vp K v)$
 ⟨proof⟩

2.5 pow of vp and n -value – convergence –

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

⟨proof⟩

lemma (in *Corps*) n -value- x -1-nat: $\llbracket \text{valuation } K v; x \in (vp K v) \diamond (Vr K v) n \rrbracket \implies (an n) \leq (n\text{-val } K v x)$

⟨proof⟩

lemma (in *Corps*) n -value- x -2: $\llbracket \text{valuation } K v; x \in \text{carrier } (Vr K v); n \leq (n\text{-val } K v x); 0 \leq n \rrbracket \implies x \in (vp K v) (Vr K v) n$

⟨proof⟩

lemma (in *Corps*) n -value- x -2-nat: $\llbracket \text{valuation } K v; x \in \text{carrier } (Vr K v); (an n) \leq ((n\text{-val } K v) x) \rrbracket \implies x \in (vp K v) \diamond (Vr K v) n$

⟨proof⟩

lemma (in *Corps*) n -val- n -pow: $\llbracket \text{valuation } K v; x \in \text{carrier } (Vr K v); 0 \leq n \rrbracket \implies (n \leq (n\text{-val } K v x)) = (x \in (vp K v) (Vr K v) n)$

⟨proof⟩

lemma (in *Corps*) equal-in-vpr-apow : $\llbracket \text{valuation } K v; x \in \text{carrier } K; 0 \leq n; y \in \text{carrier } K; n\text{-val } K v x = n\text{-val } K v y; x \in (vp K v) (Vr K v) n \rrbracket \implies y \in (vp K v) (Vr K v) n$

⟨proof⟩

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

⟨proof⟩

lemma (in *Corps*) convergenceTr1 : $\llbracket \text{valuation } K v; x \in \text{carrier } K; b \in (vp K v) (Vr K v) (n + Abs (n\text{-val } K v x)); 0 \leq n \rrbracket \implies x \cdot_r b \in (vp K v) (Vr K v) n$

⟨proof⟩

lemma (in *Corps*) vp-potent-zero : $\llbracket \text{valuation } K v; 0 \leq n \rrbracket \implies (n = \infty) = (vp K v (Vr K v) n = \{\mathbf{0}_{Vr K v}\})$

⟨proof⟩

lemma (in Corps) Vr-potent-eqTr1: $\llbracket \text{valuation } K v; 0 \leq n; 0 \leq m; (vp K v) (Vr K v) n = (vp K v) (Vr K v) m, m = 0 \rrbracket \implies n = m$

$\langle \text{proof} \rangle$

lemma (in Corps) Vr-potent-eqTr2: $\llbracket \text{valuation } K v; (vp K v) \diamond (Vr K v) n = (vp K v) \diamond (Vr K v) m \rrbracket \implies n = m$

$\langle \text{proof} \rangle$

lemma (in Corps) Vr-potent-eq: $\llbracket \text{valuation } K v; 0 \leq n; 0 \leq m; (vp K v) (Vr K v) n = (vp K v) (Vr K v) m \rrbracket \implies n = m$

$\langle \text{proof} \rangle$

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

lemma (in Corps) Vr-prime-maximalTr1: $\llbracket \text{valuation } K v; x \in \text{carrier } (Vr K v); Suc\ 0 < n \rrbracket \implies x \cdot_r (Vr K v) (x^{K (n - Suc\ 0)}) \in (Vr K v) \diamond_p (x^{K n})$

$\langle \text{proof} \rangle$

lemma (in Corps) Vr-prime-maximalTr2: $\llbracket \text{valuation } K v; x \in vp\ K\ v; x \neq \mathbf{0}; Suc\ 0 < n \rrbracket \implies x \notin Vr\ K\ v \diamond_p (x^{K n}) \wedge x^{K (n - Suc\ 0)} \notin (Vr K v) \diamond_p (x^{K n})$

$\langle \text{proof} \rangle$

lemma (in Corps) Vring-prime-maximal: $\llbracket \text{valuation } K v; \text{prime-ideal } (Vr K v) I; I \neq \{\mathbf{0}_{Vr K v}\} \rrbracket \implies \text{maximal-ideal } (Vr K v) I$

$\langle \text{proof} \rangle$

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

lemma (in Corps) field-frac1: $\llbracket 1_r \neq \mathbf{0}; x \in \text{carrier } K \rrbracket \implies x = x \cdot_r ((1_r)^{-K})$

$\langle \text{proof} \rangle$

lemma (in Corps) field-frac2: $\llbracket x \in \text{carrier } K; x \neq \mathbf{0} \rrbracket \implies x = (1_r) \cdot_r ((x^{-K})^{-K})$

$\langle \text{proof} \rangle$

lemma (in Corps) val-nonpos-inv-pos: $\llbracket \text{valuation } K v; x \in \text{carrier } K; \neg 0 \leq (v x) \rrbracket \implies 0 < (v (x^{-K}))$

$\langle \text{proof} \rangle$

lemma (in Corps) frac-Vr-is-K: $\llbracket \text{valuation } K v; x \in \text{carrier } K \rrbracket \implies \exists s \in \text{carrier } (Vr K v). \exists t \in \text{carrier } (Vr K v) - \{\mathbf{0}\}. x = s \cdot_r (t^{-K})$

$\langle \text{proof} \rangle$

lemma (in Corps) valuations-eqTr1: $\llbracket \text{valuation } K v; \text{valuation } K v' \rrbracket$

$Vr K v = Vr K v'; \forall x \in carrier (Vr K v). v x = v' x \implies v = v'$
 ⟨proof⟩

lemma (in Corps) *ridmap-rhom*: $[[valuation K v; valuation K v';$
 $carrier (Vr K v) \subseteq carrier (Vr K v')]] \implies$
 $ridmap (Vr K v) \in rHom (Vr K v) (Vr K v')$
 ⟨proof⟩

lemma (in Corps) *contract-ideal*: $[[valuation K v; valuation K v';$
 $carrier (Vr K v) \subseteq carrier (Vr K v')]] \implies$
 $ideal (Vr K v) (carrier (Vr K v) \cap vp K v')$
 ⟨proof⟩

lemma (in Corps) *contract-prime*: $[[valuation K v; valuation K v';$
 $carrier (Vr K v) \subseteq carrier (Vr K v')]] \implies$
 $prime-ideal (Vr K v) (carrier (Vr K v) \cap vp K v')$
 ⟨proof⟩

lemma (in Corps) *valuation-equivTr*: $[[valuation K v; valuation K v';$
 $x \in carrier K; 0 < (v' x); carrier (Vr K v) \subseteq carrier (Vr K v')]]$
 $\implies 0 \leq (v x)$
 ⟨proof⟩

lemma (in Corps) *contract-maximal*: $[[valuation K v; valuation K v';$
 $carrier (Vr K v) \subseteq carrier (Vr K v')]] \implies$
 $maximal-ideal (Vr K v) (carrier (Vr K v) \cap vp K v')$
 ⟨proof⟩

2.6 Equivalent valuations

definition

$v\text{-equiv} :: [-, 'r \Rightarrow ant, 'r \Rightarrow ant] \Rightarrow bool$ **where**
 $v\text{-equiv } K v1 v2 \longleftrightarrow n\text{-val } K v1 = n\text{-val } K v2$

lemma (in Corps) *valuation-equivTr1*: $[[valuation K v; valuation K v';$
 $\forall x \in carrier K. 0 \leq (v x) \longrightarrow 0 \leq (v' x)]] \implies$
 $carrier (Vr K v) \subseteq carrier (Vr K v')$
 ⟨proof⟩

lemma (in Corps) *valuation-equivTr2*: $[[valuation K v; valuation K v';$
 $carrier (Vr K v) \subseteq carrier (Vr K v'); vp K v = carrier (Vr K v) \cap vp K v']]$
 $\implies carrier (Vr K v') \subseteq carrier (Vr K v)$
 ⟨proof⟩

lemma (in Corps) *eq-carr-eq-Vring*: $[[valuation K v; valuation K v';$
 $carrier (Vr K v) = carrier (Vr K v')]] \implies Vr K v = Vr K v'$
 ⟨proof⟩

lemma (in Corps) *valuations-equiv*: \llbracket valuation K v ; valuation K v' ;
 $\forall x \in \text{carrier } K. 0 \leq (v x) \longrightarrow 0 \leq (v' x)\rrbracket \implies v\text{-equiv } K v v'$

$\langle \text{proof} \rangle$

lemma (in Corps) *val-equiv-axiom1*: \llbracket valuation K $v \rrbracket \implies v\text{-equiv } K v v$

$\langle \text{proof} \rangle$

lemma (in Corps) *val-equiv-axiom2*: \llbracket valuation K v ; valuation K v' ;
 $v\text{-equiv } K v v' \rrbracket \implies v\text{-equiv } K v' v$

$\langle \text{proof} \rangle$

lemma (in Corps) *val-equiv-axiom3*: \llbracket valuation K v ; valuation K v' ;
valuation K v' ; $v\text{-equiv } K v v'$; $v\text{-equiv } K v' v'' \rrbracket \implies v\text{-equiv } K v v''$

$\langle \text{proof} \rangle$

lemma (in Corps) *n-val-equiv-val*: \llbracket valuation K $v \rrbracket \implies$
 $v\text{-equiv } K v (n\text{-val } K v)$

$\langle \text{proof} \rangle$

2.7 Prime divisors

definition

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

definition

prime-divisors :: $- \Rightarrow ('b \Rightarrow \text{ant}) \text{ set set } (Pds_1 96) \text{ where}$
 $Pds_K = \{P. \exists v. \text{valuation } K v \wedge P = P_K v \}$

definition

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

lemma (in Corps) *val-in-P-valuation*: \llbracket valuation K v ; $v' \in P_K v \rrbracket \implies$
 $\text{valuation } K v'$

$\langle \text{proof} \rangle$

lemma (in Corps) *vals-in-P-equiv*: \llbracket valuation K v ; $v' \in P_K v \rrbracket \implies$
 $v\text{-equiv } K v v'$

$\langle \text{proof} \rangle$

lemma (in Corps) *v-in-prime-v*: $\text{valuation } K v \implies v \in P_K v$

$\langle \text{proof} \rangle$

lemma (in Corps) *some-in-prime-divisor*: $\text{valuation } K v \implies$

$(\text{SOME } w. w \in P_K v) \in P_K v$
 ⟨proof⟩

lemma (in Corps) valuation-some-in-prime-divisor: valuation $K v$
 \implies valuation $K (\text{SOME } w. w \in P_K v)$
 ⟨proof⟩

lemma (in Corps) valuation-some-in-prime-divisor1: $P \in Pds \implies$
 valuation $K (\text{SOME } w. w \in P)$
 ⟨proof⟩

lemma (in Corps) representative-of-pd-valuation:
 $P \in Pds \implies$ valuation $K (\nu_K P)$
 ⟨proof⟩

lemma (in Corps) some-in-P-equiv: valuation $K v \implies$
 $v\text{-equiv } K v (\text{SOME } w. w \in P_K v)$
 ⟨proof⟩

lemma (in Corps) n-val-n-val1: $P \in Pds \implies n\text{-val } K (\nu_K P) = (\nu_K P)$
 ⟨proof⟩

lemma (in Corps) P-eq-val-equiv: \llbracket valuation $K v$; valuation $K v' \rrbracket \implies$
 $(v\text{-equiv } K v v') = (P_K v = P_K v')$
 ⟨proof⟩

lemma (in Corps) unique-n-valuation: $\llbracket P \in Pds_K; P' \in Pds \rrbracket \implies$
 $(P = P') = (\nu_K P = \nu_K P')$
 ⟨proof⟩

lemma (in Corps) n-val-representative: $P \in Pds \implies (\nu_K P) \in P$
 ⟨proof⟩

lemma (in Corps) val-equiv-eq-pdiv: $\llbracket P \in Pds_K; P' \in Pds_K; \text{valuation } K v$;
 valuation $K v'$; $v\text{-equiv } K v v'$; $v \in P$; $v' \in P' \rrbracket \implies P = P'$
 ⟨proof⟩

lemma (in Corps) distinct-p-divisors: $\llbracket P \in Pds_K; P' \in Pds_K \rrbracket \implies$
 $(\neg P = P') = (\neg v\text{-equiv } K (\nu_K P) (\nu_K P'))$
 ⟨proof⟩

2.8 Approximation

definition

valuations :: $[-, \text{nat}, \text{nat} \Rightarrow ('r \Rightarrow \text{ant})] \Rightarrow \text{bool}$ **where**
 valuations $K n vv \iff (\forall j \leq n. \text{valuation } K (vv j))$

definition

vals-nonequiv :: $[-, \text{nat}, \text{nat} \Rightarrow ('r \Rightarrow \text{ant})] \Rightarrow \text{bool}$ **where**

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

definition

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

lemma (in *Corps*) $Ostrowski\text{-}elem\ 0$: $\llbracket vals\text{-}nonequiv\ K\ n\ vv; x \in carrier\ K; Ostrowski\text{-}elem\ K\ n\ vv\ x \rrbracket \Longrightarrow 0 < (vv\ 0\ (1_r \pm (-_a\ x)))$
 $\langle proof \rangle$

lemma (in *Corps*) $Ostrowski\text{-}elem\ Suc$: $\llbracket vals\text{-}nonequiv\ K\ n\ vv; x \in carrier\ K; Ostrowski\text{-}elem\ K\ n\ vv\ x; j \in nset\ (Suc\ 0)\ n \rrbracket \Longrightarrow 0 < (vv\ j\ x)$
 $\langle proof \rangle$

lemma (in *Corps*) $vals\text{-}nonequiv\text{-}valuation$: $\llbracket vals\text{-}nonequiv\ K\ n\ vv; m \leq n \rrbracket \Longrightarrow valuation\ K\ (vv\ m)$
 $\langle proof \rangle$

lemma (in *Corps*) $vals\text{-}nonequiv$: $\llbracket vals\text{-}nonequiv\ K\ (Suc\ (Suc\ n))\ vv; i \leq (Suc\ (Suc\ n)); j \leq (Suc\ (Suc\ n)); i \neq j \rrbracket \Longrightarrow \neg (v\text{-equiv}\ K\ (vv\ i)\ (vv\ j))$
 $\langle proof \rangle$

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

lemma (in *Corps*) $not\text{-}v\text{-equiv}\text{-}reflex$: $\llbracket valuation\ K\ v; valuation\ K\ v'; \neg v\text{-equiv}\ K\ v\ v' \rrbracket \Longrightarrow \neg v\text{-equiv}\ K\ v'\ v$
 $\langle proof \rangle$

lemma (in *Corps*) $nonequiv\text{-}ex\text{-}Ostrowski\text{-}elem$: $\llbracket valuation\ K\ v; valuation\ K\ v'; \neg v\text{-equiv}\ K\ v\ v' \rrbracket \Longrightarrow \exists x \in carrier\ K. 0 \leq (v\ x) \wedge (v'\ x) < 0$
 $\langle proof \rangle$

lemma (in *Corps*) $field\text{-}op\text{-}minus$: $\llbracket a \in carrier\ K; b \in carrier\ K; b \neq 0 \rrbracket \Longrightarrow -_a\ (a \cdot_r (b^{-K})) = (-_a\ a) \cdot_r (b^{-K})$
 $\langle proof \rangle$

lemma (in *Corps*) $field\text{-}one\text{-}plus\text{-}frac1$: $\llbracket a \in carrier\ K; b \in carrier\ K; b \neq 0 \rrbracket \Longrightarrow 1_r \pm (a \cdot_r (b^{-K})) = (b \pm a) \cdot_r (b^{-K})$
 $\langle proof \rangle$

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

<proof>

lemma (in Corps) *field-one-plus-frac3*: $\llbracket x \in \text{carrier } K; x \neq 1_r;$

$$1_r \pm x \cdot_r (1_r \pm -_a x) \neq \mathbf{0} \rrbracket \implies$$

$$1_r \pm -_a x \cdot_r (1_r \pm x \cdot_r (1_r \pm -_a x))^{-K} =$$

$$(1_r \pm -_a x \cdot_r (Suc (Suc 0))) \cdot_r (1_r \pm x \cdot_r (1_r \pm -_a x))^{-K}$$

<proof>

lemma (in Corps) *OstrowskiTr1*: $\llbracket \text{valuation } K v; s \in \text{carrier } K; t \in \text{carrier } K;$

$$0 \leq (v s); v t < 0 \rrbracket \implies s \pm t \neq \mathbf{0}$$

<proof>

lemma (in Corps) *OstrowskiTr2*: $\llbracket \text{valuation } K v; s \in \text{carrier } K; t \in \text{carrier } K;$

$$0 \leq (v s); v t < 0 \rrbracket \implies 0 < (v (1_r \pm (-_a ((t \cdot_r ((s \pm t)^{-K}))))))$$

<proof>

lemma (in Corps) *OstrowskiTr3*: $\llbracket \text{valuation } K v; s \in \text{carrier } K; t \in \text{carrier } K;$

$$0 \leq (v t); v s < 0 \rrbracket \implies 0 < (v (t \cdot_r ((s \pm t)^{-K}))$$

<proof>

lemma (in Corps) *restrict-Ostrowski-elem*: $\llbracket x \in \text{carrier } K;$

$$\text{Ostrowski-elem } K (Suc (Suc n)) vv x \rrbracket \implies \text{Ostrowski-elem } K (Suc n) vv x$$

<proof>

lemma (in Corps) *restrict-vals-nonequiv*: $\text{vals-nonequiv } K (Suc (Suc n)) vv \implies$

$$\text{vals-nonequiv } K (Suc n) vv$$

<proof>

lemma (in Corps) *restrict-vals-nonequiv1*: $\text{vals-nonequiv } K (Suc (Suc n)) vv \implies$

$$\text{vals-nonequiv } K (Suc n) (\text{compose } \{h. h \leq (Suc n)\} vv (\text{skip } 1))$$

<proof>

lemma (in Corps) *restrict-vals-nonequiv2*: $\llbracket \text{vals-nonequiv } K (Suc (Suc n)) vv \rrbracket$

$$\implies \text{vals-nonequiv } K (Suc n) (\text{compose } \{j. j \leq (Suc n)\} vv (\text{skip } 2))$$

<proof>

lemma (in Corps) *OstrowskiTr31*: $\llbracket \text{valuation } K v; s \in \text{carrier } K;$

$$0 < (v (1_r \pm (-_a s))) \rrbracket \implies s \neq \mathbf{0}$$

<proof>

lemma (in Corps) *OstrowskiTr32*: $\llbracket \text{valuation } K v; s \in \text{carrier } K;$

$$0 < (v (1_r \pm (-_a s))) \rrbracket \implies 0 \leq (v s)$$

<proof>

lemma (in Corps) *OstrowskiTr4*: $\llbracket \text{valuation } K v; s \in \text{carrier } K; t \in \text{carrier } K;$

$$0 < (v (1_r \pm (-_a s))); 0 < (v (1_r \pm (-_a t))) \rrbracket \implies$$

$$0 < (v (1_r \pm (-_a (s \cdot_r t))))$$

<proof>

lemma (in Corps) OstrowskiTr5: $\llbracket \text{vals-nonequiv } K \text{ (Suc (Suc } n)) \text{ } vv;$
 $s \in \text{carrier } K; t \in \text{carrier } K;$
 $0 \leq (vv \text{ (Suc } 0)) \text{ } s \wedge 0 \leq (vv \text{ (Suc (Suc } 0))) \text{ } t;$
 $\text{Ostrowski-elem } K \text{ (Suc } n) \text{ (compose } \{j. j \leq (\text{Suc } n)\} \text{ } vv \text{ (skip } 1)) \text{ } s;$
 $\text{Ostrowski-elem } K \text{ (Suc } n) \text{ (compose } \{j. j \leq (\text{Suc } n)\} \text{ } vv \text{ (skip } 2)) \text{ } t \rrbracket \implies$
 $\text{Ostrowski-elem } K \text{ (Suc (Suc } n)) \text{ } vv \text{ (s } \cdot_r \text{ t)}$
 <proof>

lemma (in Corps) one-plus-x-nonzero: $\llbracket \text{valuation } K \text{ } v; x \in \text{carrier } K; v \text{ } x < 0 \rrbracket$
 $\implies 1_r \pm x \in \text{carrier } K \wedge v \text{ (} 1_r \pm x) < 0$
 <proof>

lemma (in Corps) val-neg-nonzero: $\llbracket \text{valuation } K \text{ } v; x \in \text{carrier } K; v \text{ } x < 0 \rrbracket \implies$
 $x \neq \mathbf{0}$
 <proof>

lemma (in Corps) OstrowskiTr6: $\llbracket \text{valuation } K \text{ } v; x \in \text{carrier } K; \neg 0 \leq (v \text{ } x) \rrbracket \implies$
 $(1_r \pm x \cdot_r (1_r \pm -_a x)) \in \text{carrier } K - \{\mathbf{0}\}$
 <proof>

lemma (in Corps) OstrowskiTr7: $\llbracket \text{valuation } K \text{ } v; x \in \text{carrier } K; \neg 0 \leq (v \text{ } x) \rrbracket \implies$
 $1_r \pm -_a (x \cdot_r ((1_r \pm x \cdot_r (1_r \pm -_a x))^{-K})) =$
 $(1_r \pm -_a x \pm x \cdot_r (1_r \pm -_a x)) \cdot_r ((1_r \pm x \cdot_r (1_r \pm -_a x))^{-K})$
 <proof>

lemma (in Corps) Ostrowski-elem-nonzero: $\llbracket \text{vals-nonequiv } K \text{ (Suc } n) \text{ } vv;$
 $x \in \text{carrier } K; \text{Ostrowski-elem } K \text{ (Suc } n) \text{ } vv \text{ } x \rrbracket \implies x \neq \mathbf{0}$
 <proof>

lemma (in Corps) Ostrowski-elem-not-one: $\llbracket \text{vals-nonequiv } K \text{ (Suc } n) \text{ } vv;$
 $x \in \text{carrier } K; \text{Ostrowski-elem } K \text{ (Suc } n) \text{ } vv \text{ } x \rrbracket \implies 1_r \pm -_a x \neq \mathbf{0}$
 <proof>

lemma (in Corps) val-unit-cond: $\llbracket \text{valuation } K \text{ } v; x \in \text{carrier } K;$
 $0 < (v \text{ (} 1_r \pm -_a x)) \rrbracket \implies v \text{ } x = 0$
 <proof>

end

theory Valuation2
imports Valuation1
begin

lemma (in Corps) OstrowskiTr8: $\llbracket \text{valuation } K \text{ } v; x \in \text{carrier } K;$
 $0 < v \text{ (} 1_r \pm -_a x) \rrbracket \implies$
 $0 < (v \text{ (} 1_r \pm -_a (x \cdot_r ((1_r \pm x \cdot_r (1_r \pm -_a x))^{-K}))))$
 <proof>

lemma (in Corps) OstrowskiTr9: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K; 0 < (v \ x) \rrbracket \implies$
 $0 < (v \ (x \cdot_r \ ((1_r \pm x \cdot_r \ (1_r \pm -_a \ x))^{-K})))$

$\langle \text{proof} \rangle$

lemma (in Corps) OstrowskiTr10: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K;$
 $\neg 0 \leq v \ x \rrbracket \implies 0 < (v \ (x \cdot_r \ ((1_r \pm x \cdot_r \ (1_r \pm -_a \ x))^{-K})))$

$\langle \text{proof} \rangle$

lemma (in Corps) Ostrowski-first:vals-nonequiv K (Suc 0) vv
 $\implies \exists x \in \text{carrier } K. \text{Ostrowski-elem } K \ (Suc \ 0) \ vv \ x$

$\langle \text{proof} \rangle$

lemma (in Corps) Ostrowski: $\forall vv. \text{vals-nonequiv } K \ (Suc \ n) \ vv \longrightarrow$
 $(\exists x \in \text{carrier } K. \text{Ostrowski-elem } K \ (Suc \ n) \ vv \ x)$

$\langle \text{proof} \rangle$

lemma (in Corps) val-1-nonzero: $\llbracket \text{valuation } K \ v; x \in \text{carrier } K; v \ x = 1 \rrbracket \implies$
 $x \neq \mathbf{0}$

$\langle \text{proof} \rangle$

lemma (in Corps) Approximation1-5Tr1: $\llbracket \text{vals-nonequiv } K \ (Suc \ n) \ vv;$
 $n\text{-val } K \ (vv \ 0) = vv \ 0; a \in \text{carrier } K; vv \ 0 \ a = 1; x \in \text{carrier } K;$
 $\text{Ostrowski-elem } K \ (Suc \ n) \ vv \ x \rrbracket \implies$

$$\forall m. 2 \leq m \longrightarrow vv \ 0 \ ((1_r \pm -_a \ x) \wedge^K m \pm a \cdot_r (x \wedge^K m)) = 1$$

$\langle \text{proof} \rangle$

lemma (in Corps) Approximation1-5Tr3: $\llbracket \text{vals-nonequiv } K \ (Suc \ n) \ vv;$
 $x \in \text{carrier } K; \text{Ostrowski-elem } K \ (Suc \ n) \ vv \ x; j \in \text{nset } (Suc \ 0) \ (Suc \ n) \rrbracket$

$$\implies vv \ j \ ((1_r \pm -_a \ x) \wedge^K m) = 0$$

$\langle \text{proof} \rangle$

lemma (in Corps) Approximation1-5Tr4: $\llbracket \text{vals-nonequiv } K \ (Suc \ n) \ vv;$
 $aa \in \text{carrier } K; x \in \text{carrier } K;$

$$\text{Ostrowski-elem } K \ (Suc \ n) \ vv \ x; j \leq (Suc \ n) \rrbracket \implies$$

$$vv \ j \ (aa \cdot_r (x \wedge^K m)) = vv \ j \ aa + (int \ m) *_a (vv \ j \ x)$$

$\langle \text{proof} \rangle$

lemma (in Corps) Approximation1-5Tr5: $\llbracket \text{vals-nonequiv } K \ (Suc \ n) \ vv;$
 $a \in \text{carrier } K; a \neq \mathbf{0}; x \in \text{carrier } K;$

$$\text{Ostrowski-elem } K \ (Suc \ n) \ vv \ x; j \in \text{nset } (Suc \ 0) \ (Suc \ n) \rrbracket \implies$$

$$\exists l. \forall m. l < m \longrightarrow 0 < (vv \ j \ (a \cdot_r (x \wedge^K m)))$$

$\langle \text{proof} \rangle$

lemma (in Corps) Approximation1-5Tr6: $\llbracket \text{vals-nonequiv } K \ (Suc \ n) \ vv;$
 $a \in \text{carrier } K; a \neq \mathbf{0}; x \in \text{carrier } K;$

$$\text{Ostrowski-elem } K \ (Suc \ n) \ vv \ x; j \in \text{nset } (Suc \ 0) \ (Suc \ n) \rrbracket \implies$$

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

lemma (in Corps) *Approximation1-5Tr7*: $\llbracket a \in \text{carrier } K; vv\ 0\ a = 1;$
 $x \in \text{carrier } K \rrbracket \Longrightarrow$
 $\text{vals-nonequiv } K\ (Suc\ n)\ vv \wedge \text{Ostrowski-elem } K\ (Suc\ n)\ vv\ x \longrightarrow$
 $(\exists l. \forall m. l < m \longrightarrow (\forall j \in \text{nset } (Suc\ 0)\ (Suc\ n)).$
 $(vv\ j\ ((1_r \pm -_a\ x)^{\wedge K\ m} \pm a \cdot_r (x^{\wedge K\ m})) = 0)))$
 ⟨proof⟩

lemma (in Corps) *Approximation1-5P*: $\llbracket \text{vals-nonequiv } K\ (Suc\ n)\ vv;$
 $n\text{-val } K\ (vv\ 0) = vv\ 0 \rrbracket \Longrightarrow$
 $\exists x \in \text{carrier } K. ((vv\ 0\ x = 1) \wedge (\forall j \in \text{nset } (Suc\ 0)\ (Suc\ n). (vv\ j\ x) = 0))$
 ⟨proof⟩

lemma *K-gamma-hom*: $k \leq n \Longrightarrow \forall j \leq n. (\lambda l. \gamma_k\ l)\ j \in Zset$
 ⟨proof⟩

lemma *transpos-eq*: $(\tau_0\ 0)\ k = k$
 ⟨proof⟩

lemma (in Corps) *transpos-vals-nonequiv*: $\llbracket \text{vals-nonequiv } K\ (Suc\ n)\ vv;$
 $j \leq (Suc\ n) \rrbracket \Longrightarrow \text{vals-nonequiv } K\ (Suc\ n)\ (vv \circ (\tau_0\ j))$
 ⟨proof⟩

definition

Ostrowski-base :: $[-, \text{nat} \Rightarrow 'b \Rightarrow \text{ant}, \text{nat}] \Rightarrow (\text{nat} \Rightarrow 'b)$
 $((\Omega\ _ _)\ [90,90,91]90)$ **where**
Ostrowski-base $K\ vv\ n = (\lambda j \in \{h. h \leq n\}. (\text{SOME } x. x \in \text{carrier } K \wedge$
 $(\text{Ostrowski-elem } K\ n\ (vv \circ (\tau_0\ j))\ x)))$

definition

App-base :: $[-, \text{nat} \Rightarrow 'b \Rightarrow \text{ant}, \text{nat}] \Rightarrow (\text{nat} \Rightarrow 'b)$ **where**
App-base $K\ vv\ n = (\lambda j \in \{h. h \leq n\}. (\text{SOME } x. x \in \text{carrier } K \wedge (((vv \circ \tau_0\ j)\ 0\ x$
 $= 1) \wedge (\forall k \in \text{nset } (Suc\ 0)\ n. ((vv \circ \tau_0\ j)\ k\ x) = 0))))$

lemma (in Corps) *Ostrowski-base-hom*: $\text{vals-nonequiv } K\ (Suc\ n)\ vv \Longrightarrow$
 $\text{Ostrowski-base } K\ vv\ (Suc\ n) \in \{h. h \leq (Suc\ n)\} \rightarrow \text{carrier } K$
 ⟨proof⟩

lemma (in Corps) *Ostrowski-base-mem*: $\text{vals-nonequiv } K\ (Suc\ n)\ vv \Longrightarrow$
 $\forall j \leq (Suc\ n). \text{Ostrowski-base } K\ vv\ (Suc\ n)\ j \in \text{carrier } K$
 ⟨proof⟩

lemma (in Corps) *Ostrowski-base-mem-1*: $\llbracket \text{vals-nonequiv } K\ (Suc\ n)\ vv;$
 $j \leq (Suc\ n) \rrbracket \Longrightarrow \text{Ostrowski-base } K\ vv\ (Suc\ n)\ j \in \text{carrier } K$
 ⟨proof⟩

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

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

lemma (in Corps) *App-base-hom*: $\llbracket \text{vals-nonequiv } K \text{ (Suc } n) \text{ } vv; \forall j \leq \text{Suc } n. n\text{-val } K \text{ (} vv \ j) = vv \ j \rrbracket \implies \forall j \leq \text{Suc } n. \text{App-base } K \text{ } vv \text{ (Suc } n) \ j \in \text{carrier } K$
 ⟨proof⟩

lemma (in Corps) *Approximation1-5P2*: $\llbracket \text{vals-nonequiv } K \text{ (Suc } n) \text{ } vv; \forall l \in \{h. h \leq \text{Suc } n\}. n\text{-val } K \text{ (} vv \ l) = vv \ l; i \leq \text{Suc } n; j \leq \text{Suc } n \rrbracket \implies vv \ i \text{ (App-base } K \text{ } vv \text{ (Suc } n) \ j) = \delta_{i \ j}$
 ⟨proof⟩

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

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

lemma (in Corps) *Ostrowski-baseTr1*: $\llbracket \text{vals-nonequiv } K \text{ (Suc } n) \text{ } vv; l \leq \text{Suc } n \rrbracket \implies 0 < ((vv \ l) (1_r \pm -_a (\text{Ostrowski-base } K \text{ } vv \text{ (Suc } n) \ l)))$
 ⟨proof⟩

lemma (in Corps) *Ostrowski-baseTr2*: $\llbracket \text{vals-nonequiv } K \text{ (Suc } n) \text{ } vv; l \leq \text{Suc } n; m \leq \text{Suc } n; l \neq m \rrbracket \implies 0 < ((vv \ m) (\text{Ostrowski-base } K \text{ } vv \text{ (Suc } n) \ l))$
 ⟨proof⟩

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

lemma (in Corps) *Ostrowski-base-mpow-not-one*: $\llbracket 0 < N; j \leq \text{Suc } n; \text{vals-nonequiv } K \text{ (Suc } n) \text{ } vv \rrbracket \implies 1_r \pm -_a ((\Omega_{K \text{ } vv} \text{ (Suc } n)) j^{\wedge K \ N}) \neq \mathbf{0}$
 ⟨proof⟩

abbreviation

CHOOSE :: [nat, nat] \Rightarrow nat ((-C-) [80, 81]80) **where**
 $nC_i == n \text{ choose } i$

lemma (in Ring) *expansion-of-sum1*: $x \in \text{carrier } R \implies$
 $(1_r \pm x) \wedge^R n = \text{nsum } R (\lambda i. nC_i \times_R x \wedge^R i) n$
 <proof>

lemma (in Ring) *tail-of-expansion*: $x \in \text{carrier } R \implies (1_r \pm x) \wedge^R (\text{Suc } n) =$
 $(\text{nsum } R (\lambda i. ((\text{Suc } n) C (\text{Suc } i) \times_R x \wedge^R (\text{Suc } i))) n) \pm 1_r$
 <proof>

lemma (in Ring) *tail-of-expansion1*: $x \in \text{carrier } R \implies$
 $(1_r \pm x) \wedge^R (\text{Suc } n) = x \cdot_r (\text{nsum } R (\lambda i. ((\text{Suc } n) C (\text{Suc } i) \times_R x \wedge^R i)) n) \pm 1_r$
 <proof>

lemma (in Corps) *nsum-in-VrTr:valuation K v* \implies
 $(\forall j \leq n. f j \in \text{carrier } K) \wedge (\forall j \leq n. 0 \leq (v (f j))) \longrightarrow (\text{nsum } K f n) \in \text{carrier } (\text{Vr } K v)$
 <proof>

lemma (in Corps) *nsum-in-Vr:valuation K v; $\forall j \leq n. f j \in \text{carrier } K;$*
 $\forall j \leq n. 0 \leq (v (f j)) \implies (\text{nsum } K f n) \in \text{carrier } (\text{Vr } K v)$
 <proof>

lemma (in Corps) *nsum-mem-in-Vr:valuation K v;*
 $\forall j \leq n. (f j) \in \text{carrier } K; \forall j \leq n. 0 \leq (v (f j)) \implies$
 $(\text{nsum } K f n) \in \text{carrier } (\text{Vr } K v)$
 <proof>

lemma (in Corps) *val-nscal-ge-selfTr:valuation K v; $x \in \text{carrier } K; 0 \leq v x$*
 $\implies v x \leq v (n \times_K x)$
 <proof>

lemma (in Corps) *ApproximationTr:valuation K v; $x \in \text{carrier } K; 0 \leq (v x)$*
 \implies
 $v x \leq (v (1_r \pm -_a ((1_r \pm x) \wedge^K (\text{Suc } n))))$
 <proof>

lemma (in Corps) *ApproximationTr0:aa $\in \text{carrier } K \implies$*
 $(1_r \pm -_a (aa \wedge^K N)) \wedge^K N \in \text{carrier } K$
 <proof>

lemma (in Corps) *ApproximationTr1:aa $\in \text{carrier } K \implies$*
 $1_r \pm -_a ((1_r \pm -_a (aa \wedge^K N)) \wedge^K N) \in \text{carrier } K$
 <proof>

lemma (in Corps) *ApproximationTr2:valuation K v; aa $\in \text{carrier } K; aa \neq \mathbf{0};$*
 $0 \leq (v aa) \implies (\text{int } N) *_a (v aa) \leq (v (1_r \pm -_a ((1_r \pm -_a (aa \wedge^K N)) \wedge^K N)))$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *eSum-tr*:

$$\begin{aligned} & (\forall j \leq n. (x j) \in \text{carrier } K) \wedge \\ & (\forall j \leq n. (b j) \in \text{carrier } K) \wedge l \leq n \wedge \\ & (\forall j \in (\{h. h \leq n\} - \{l\}). (g j = (x j) \cdot_r (1_r \pm_{-a} (b j)))) \wedge \\ & g l = (x l) \cdot_r (-_a (b l)) \\ \longrightarrow & (\text{nsum } K (\lambda j \in \{h. h \leq n\}. (x j) \cdot_r (1_r \pm_{-a} (b j))) n) \pm_{-a} (x l) = \\ & \text{nsum } K g n \end{aligned}$$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *eSum-minus-x*: $\llbracket \forall j \leq n. (x j) \in \text{carrier } K;$

$$\begin{aligned} & \forall j \leq n. (b j) \in \text{carrier } K; l \leq n; \\ & \forall j \in (\{h. h \leq n\} - \{l\}). (g j = (x j) \cdot_r (1_r \pm_{-a} (b j))); \\ & g l = (x l) \cdot_r (-_a (b l)) \rrbracket \Longrightarrow \\ & (\text{nsum } K (\lambda j \in \{h. h \leq n\}. (x j) \cdot_r (1_r \pm_{-a} (b j))) n) \pm_{-a} (x l) = \\ & \text{nsum } K g n \end{aligned}$$

$\langle \text{proof} \rangle$

lemma (in *Ring*) *one-m-x-times*: $x \in \text{carrier } R \Longrightarrow$

$$(1_r \pm_{-a} x) \cdot_r (\text{nsum } R (\lambda j. x^R j) n) = 1_r \pm_{-a} (x^R (\text{Suc } n))$$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *x-pow-fSum-in-Vr*: $\llbracket \text{valuation } K v; x \in \text{carrier } (Vr K v) \rrbracket \Longrightarrow$

$$(\text{nsum } K (\text{npow } K x) n) \in \text{carrier } (Vr K v)$$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-1mx-pos*: $\llbracket \text{valuation } K v; x \in \text{carrier } K;$

$$0 < (v (1_r \pm_{-a} x)) \rrbracket \Longrightarrow v x = 0$$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *val-1mx-pow*: $\llbracket \text{valuation } K v; x \in \text{carrier } K;$

$$0 < (v (1_r \pm_{-a} x)) \rrbracket \Longrightarrow 0 < (v (1_r \pm_{-a} x^K (\text{Suc } n)))$$

$\langle \text{proof} \rangle$

lemma (in *Corps*) *ApproximationTr3*: $\llbracket \text{vals-nonequiv } K (\text{Suc } n) vv;$

$$\begin{aligned} & \forall l \leq (\text{Suc } n). x l \in \text{carrier } K; j \leq (\text{Suc } n) \rrbracket \Longrightarrow \\ & \exists L. (\forall N. L < N \longrightarrow (an m) \leq (vv j ((\Sigma_e K (\lambda k \in \{h. h \leq (\text{Suc } n)\}. \\ & (x k) \cdot_r (1_r \pm_{-a} ((1_r \pm_{-a} ((\Omega_K vv (\text{Suc } n)) k) \wedge^K N)) \wedge^K N))) \\ & (\text{Suc } n)) \pm_{-a} (x j)))) \end{aligned}$$

$\langle \text{proof} \rangle$

definition

$$\begin{aligned} \text{app-lb} & :: [-, \text{nat}, \text{nat} \Rightarrow 'b \Rightarrow \text{ant}, \text{nat} \Rightarrow 'b, \text{nat}] \Rightarrow \\ & (\text{nat} \Rightarrow \text{nat}) \quad ((5\Psi \dots) [98,98,98,98,99]98) \textbf{ where} \\ \Psi_{K n} & vv x m = (\lambda j \in \{h. h \leq n\}. (\text{SOME } L. (\forall N. L < N \longrightarrow \\ & (an m) \leq (vv j (\Sigma_e K (\lambda j \in \{h. h \leq n\}. (x j) \cdot_r K (1_r K \pm_K -_a K \\ & (1_r K \pm_K -_a K ((\Omega_K vv n) j) \wedge^K N) \wedge^K N)) n \pm_K -_a K (x j)))))) \end{aligned}$$

lemma (in *Corps*) *app-LB*: $\llbracket \text{vals-nonequiv } K \text{ (Suc } n) \text{ vv};$
 $\forall l \leq (\text{Suc } n). x \ l \in \text{carrier } K; j \leq (\text{Suc } n) \rrbracket \implies$
 $\forall N. (\Psi_K (\text{Suc } n) \text{ vv } x \ m) \ j < N \longrightarrow (an \ m) \leq$
 $(vv \ j \ (\Sigma_e \ K \ (\lambda j \in \{h. h \leq (\text{Suc } n)\}. (x \ j) \cdot_r (1_r \pm -_a (1_r \pm$
 $-_a ((\Omega_K \text{ vv } (\text{Suc } n)) \ j) \wedge^K N) \wedge^K N)) (\text{Suc } n) \pm -_a (x \ j)))$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *ApplicationTr4*: $\llbracket \text{vals-nonequiv } K \text{ (Suc } n) \text{ vv};$
 $\forall j \in \{h. h \leq (\text{Suc } n)\}. x \ j \in \text{carrier } K \rrbracket \implies$
 $\exists l. \forall N. l < N \longrightarrow (\forall j \leq (\text{Suc } n). (an \ m) \leq$
 $(vv \ j \ (\Sigma_e \ K \ (\lambda j \in \{h. h \leq (\text{Suc } n)\}. (x \ j) \cdot_r (1_r \pm -_a (1_r \pm$
 $-_a ((\Omega_K \text{ vv } (\text{Suc } n)) \ j) \wedge^K N) \wedge^K N)) (\text{Suc } n) \pm -_a (x \ j)))$
 $\langle \text{proof} \rangle$

theorem (in *Corps*) *Approximation-thm*: $\llbracket \text{vals-nonequiv } K \text{ (Suc } n) \text{ vv};$
 $\forall j \leq (\text{Suc } n). (x \ j) \in \text{carrier } K \rrbracket \implies$
 $\exists y \in \text{carrier } K. \forall j \leq (\text{Suc } n). (an \ m) \leq (vv \ j \ (y \pm -_a (x \ j)))$
 $\langle \text{proof} \rangle$

definition

distinct-pds :: $[-, \text{nat}, \text{nat} \Rightarrow ('b \Rightarrow \text{ant}) \text{ set}] \Rightarrow \text{bool}$ **where**
 $\text{distinct-pds } K \ n \ P \longleftrightarrow (\forall j \leq n. P \ j \in \text{Pds } K) \wedge$
 $(\forall l \leq n. \forall m \leq n. l \neq m \longrightarrow P \ l \neq P \ m)$

lemma (in *Corps*) *distinct-pds-restriction*: $\llbracket \text{distinct-pds } K \text{ (Suc } n) \ P \rrbracket \implies$
 $\text{distinct-pds } K \ n \ P$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *ring-n-distinct-prime-divisors*: $\text{distinct-pds } K \ n \ P \implies$
 $\text{Ring } (\text{Sr } K \ \{x. x \in \text{carrier } K \wedge (\forall j \leq n. 0 \leq ((\nu_K (P \ j)) \ x))\})$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *distinct-pds-valuation*: $\llbracket j \leq (\text{Suc } n);$
 $\text{distinct-pds } K \text{ (Suc } n) \ P \rrbracket \implies \text{valuation } K \ (\nu_K (P \ j))$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *distinct-pds-valuation1*: $\llbracket 0 < n; j \leq n; \text{distinct-pds } K \ n \ P \rrbracket$
 $\implies \text{valuation } K \ (\nu_K (P \ j))$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *distinct-pds-valuation2*: $\llbracket j \leq n; \text{distinct-pds } K \ n \ P \rrbracket \implies$
 $\text{valuation } K \ (\nu_K (P \ j))$
 $\langle \text{proof} \rangle$

definition

ring-n-pd :: $[('b, 'm) \text{ Ring-scheme}, \text{nat} \Rightarrow ('b \Rightarrow \text{ant}) \text{ set},$

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

lemma (in Corps) ring-n-pd:distinct-pds $K n P \implies \text{Ring } (O_{K P n})$
 $\langle \text{proof} \rangle$

lemma (in Corps) ring-n-pd-Suc:distinct-pds $K (Suc n) P \implies$
 $\text{carrier } (O_{K P (Suc n)}) \subseteq \text{carrier } (O_{K P n})$
 $\langle \text{proof} \rangle$

lemma (in Corps) ring-n-pd-pOp-K-pOp: $[[\text{distinct-pds } K n P; x \in \text{carrier } (O_{K P n});$
 $y \in \text{carrier } (O_{K P n})]] \implies x \pm_{(O_{K P n})} y = x \pm y$
 $\langle \text{proof} \rangle$

lemma (in Corps) ring-n-pd-tOp-K-tOp: $[[\text{distinct-pds } K n P; x \in \text{carrier } (O_{K P n});$
 $y \in \text{carrier } (O_{K P n})]] \implies x \cdot_r (O_{K P n}) y = x \cdot_r y$
 $\langle \text{proof} \rangle$

lemma (in Corps) ring-n-eSum-K-eSumTr:distinct-pds $K n P \implies$
 $(\forall j \leq m. f j \in \text{carrier } (O_{K P n})) \longrightarrow \text{nsun } (O_{K P n}) f m = \text{nsun } K f m$
 $\langle \text{proof} \rangle$

lemma (in Corps) ring-n-eSum-K-eSum: $[[\text{distinct-pds } K n P;$
 $\forall j \leq m. f j \in \text{carrier } (O_{K P n})]] \implies \text{nsun } (O_{K P n}) f m = \text{nsun } K f m$
 $\langle \text{proof} \rangle$

lemma (in Corps) ideal-eSum-closed: $[[\text{distinct-pds } K n P; \text{ideal } (O_{K P n}) I;$
 $\forall j \leq m. f j \in I]] \implies \text{nsun } K f m \in I$
 $\langle \text{proof} \rangle$

definition

$\text{prime-n-pd} :: [-, \text{nat} \Rightarrow ('b \Rightarrow \text{ant}) \text{ set},$
 $\text{nat}, \text{nat}] \Rightarrow 'b \text{ set}$
 $((\exists P \dots) [98,98,98,99]98) \text{ where}$
 $P_{K P n j} = \{x. x \in (\text{carrier } (O_{K P n})) \wedge 0 < ((\nu_K (P j)) x)\}$

lemma (in Corps) zero-in-ring-n-pd-zero-K:distinct-pds $K n P \implies$
 $\mathbf{0}_{(O_{K P n})} = \mathbf{0}_K$
 $\langle \text{proof} \rangle$

lemma (in Corps) one-in-ring-n-pd-one-K:distinct-pds $K n P \implies$
 $1_r (O_{K P n}) = 1_r$
 $\langle \text{proof} \rangle$

lemma (in Corps) mem-ring-n-pd-mem-K: $[[\text{distinct-pds } K n P; x \in \text{carrier } (O_{K P n})]]$

$\implies x \in \text{carrier } K$
 <proof>

lemma (in Corps) ring-n-tOp-K-tOp: [[distinct-pds K n P; x ∈ carrier (O_{K P n});
 y ∈ carrier (O_{K P n})]] $\implies x \cdot_r (O_{K P n}) y = x \cdot_r y$
 <proof>

lemma (in Corps) ring-n-exp-K-exp: [[distinct-pds K n P; x ∈ carrier (O_{K P n})]]
 $\implies x \wedge^K m = x \wedge^{(O_{K P n})} m$
 <proof>

lemma (in Corps) prime-n-pd-prime: [[distinct-pds K n P; j ≤ n]] \implies
 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 ∈ carrier (O_{K P n}); y ∈ carrier (O_{K P n});
 ∀ j ≤ n. ((ν_K (P j)) x) ≤ ((ν_K (P j)) y)]] $\implies Rxa (O_{K P n}) y \subseteq Rxa (O_{K P n}) x$
 <proof>

lemma (in Corps) n-eq-val-eq-ideal: [[distinct-pds K n P; x ∈ carrier (O_{K P n});
 y ∈ carrier (O_{K P n}); ∀ j ≤ n. ((ν_K (P j)) x) = ((ν_K (P j)) y)]] \implies
 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 ∈ I ∧
 (∀ j ≤ n. (ν_K (P j)) x = LI K (ν_K (P j)) I))

definition
 mL :: [-, nat ⇒ ('r ⇒ ant) set, 'r set, nat] ⇒ int **where**
 mL K P I j = tna (LI K (ν_K (P j)) I)

lemma (in Corps) mI-vals-nonempty: [[distinct-pds K n P; ideal (O_{K P n}) I; j ≤ n]]
 $\implies (\nu_K (P j)) \text{ ' } I \neq \{\}$
 <proof>

lemma (in Corps) mI-vals-LB: [[distinct-pds K n P; ideal (O_{K P n}) I; j ≤ n]] \implies
 ((ν_K (P j)) 'I) ⊆ LBset (ant 0)
 <proof>

lemma (in Corps) mL-hom: [[distinct-pds K n P; ideal (O_{K P n}) I;
 I ≠ {0_(O_{K P n})}; I ≠ carrier (O_{K P n})]] \implies
 ∀ j ≤ n. mL K P I j ∈ Zset
 <proof>

lemma (in *Corps*) *ex-Zleast-in-mI*: \llbracket *distinct-pds* $K\ n\ P$; *ideal* $(O_{K\ P\ n})\ I$; $j \leq n$ \rrbracket
 $\implies \exists x \in I. (\nu_K (P\ j))\ x = LI\ K\ (\nu_K (P\ j))\ I$
 ⟨*proof*⟩

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

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

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

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

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

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

definition

$KbaseP :: [-, nat \Rightarrow ('r \Rightarrow ant)\ set, nat] \Rightarrow$
 $(nat \Rightarrow 'r) \Rightarrow bool$ **where**
 $KbaseP\ K\ P\ n\ f \longleftrightarrow (\forall j \leq n. f\ j \in carrier\ K) \wedge$
 $(\forall j \leq n. \forall l \leq n. (\nu_K (P\ j))\ (f\ l) = (\delta_j\ l))$

definition

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

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

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

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

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

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

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

definition

$Zl\text{-}mI :: [-, \text{nat} \Rightarrow ('b \Rightarrow \text{ant})\ \text{set}, 'b\ \text{set}]$
 $\Rightarrow \text{nat} \Rightarrow 'b\ \mathbf{where}$

$Zl\text{-}mI\ K\ P\ I\ j = (\text{SOME } x. (x \in I \wedge ((\nu_K\ (P\ j))\ x = LI\ K\ (\nu_K\ (P\ j))\ I)))$

lemma (in *Corps*) *value-Zl-mI*: $[[\text{distinct-pds } K\ n\ P; \text{ideal } (O_{K\ P\ n})\ I; j \leq n]]$
 $\implies (Zl\text{-}mI\ K\ P\ I\ j \in I) \wedge (\nu_K\ (P\ j))\ (Zl\text{-}mI\ K\ P\ I\ j) = LI\ K\ (\nu_K\ (P\ j))\ I$
 ⟨proof⟩

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

lemma (in *Corps*) *Zl-mI-mem-K*: $[[\text{distinct-pds } K\ n\ P; \text{ideal } (O_{K\ P\ n})\ I; l \leq n]]$
 $\implies (Zl\text{-}mI\ K\ P\ I\ l) \in \text{carrier } K$
 ⟨proof⟩

definition

$mprod\text{-}exp :: [-, \text{nat} \Rightarrow \text{int}, \text{nat} \Rightarrow 'b, \text{nat}]$
 $\Rightarrow 'b\ \mathbf{where}$

$mprod\text{-}exp\ K\ e\ f\ n = nprod\ K\ (\lambda j. ((f\ j)_K^{(e\ j)}))\ n$

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

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

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

lemma (in *Corps*) *mprod-memTr*:
 $(\forall j \leq n. e j \in \text{Zset}) \wedge (\forall j \leq n. f j \in ((\text{carrier } K) - \{\mathbf{0}\})) \longrightarrow$
 $(\text{mprod-exp } K e f n) \in ((\text{carrier } K) - \{\mathbf{0}\})$
 <proof>

lemma (in *Corps*) *mprod-mem*: $\llbracket \forall j \leq n. e j \in \text{Zset}; \forall j \leq n. f j \in ((\text{carrier } K) - \{\mathbf{0}\}) \rrbracket \implies$
 $(\text{mprod-exp } K e f n) \in ((\text{carrier } K) - \{\mathbf{0}\})$
 <proof>

lemma (in *Corps*) *mprod-mprodR*: $\llbracket \forall j \leq n. e j \in \text{Zset}; \forall j \leq n. 0 \leq (e j);$
 $\forall j \leq n. f j \in ((\text{carrier } K) - \{\mathbf{0}\}) \rrbracket \implies$
 $\text{mprod-exp } K e f n = \text{mprod-expR } K (\text{nat } o e) f n$
 <proof>

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

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

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

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

lemma (in *Corps*) *value-mprod-exp*: $\llbracket \text{valuation } K v; \forall j \leq n. e j \in \text{Zset};$
 $\forall j \leq n. f j \in (\text{carrier } K - \{\mathbf{0}\}) \rrbracket \implies$
 $v (\text{mprod-exp } K e f n) = \text{ASum } (\lambda j. (e j) *_a (v (f j))) n$
 <proof>

lemma (in *Corps*) *mgenerator0-1*: $\llbracket \text{distinct-pds } K (\text{Suc } n) P;$
 $\text{ideal } (O_{K P (\text{Suc } n)}) I; I \neq \{\mathbf{0}_{(O_{K P (\text{Suc } n)})}\};$
 $I \neq \text{carrier } (O_{K P (\text{Suc } n)}); j \leq (\text{Suc } n) \rrbracket \implies$
 $((\nu_K (P j)) (\text{mprod-exp } K (\text{mL } K P I) (\text{Kb}_K (\text{Suc } n) P) (\text{Suc } n))) =$
 $((\nu_K (P j)) (\text{Zl-mI } K P I j))$
 <proof>

lemma (in *Corps*) *mgenerator0-2*: $\llbracket 0 < n; \text{distinct-pds } K n P; \text{ideal } (O_{K P n}) I;$
 $I \neq \{\mathbf{0}_{(O_{K P n})}\}; I \neq \text{carrier } (O_{K P n}); j \leq n \rrbracket \implies$

$((\nu_K (P j)) (mprod-exp K (mL K P I) (Kb_{K n P} n)) = ((\nu_K (P j)) (Zl-mI K P I j))$
 ⟨proof⟩

lemma (in Corps) mgenerator1: $\llbracket distinct-pds K n P; ideal (O_{K P n}) I; I \neq \{0_{O_{K P n}}\}; I \neq carrier (O_{K P n}); j \leq n \rrbracket \implies$
 $((\nu_K (P j)) (mprod-exp K (mL K P I) (Kb_{K n P} n)) = ((\nu_K (P j)) (Zl-mI K P I j))$
 ⟨proof⟩

lemma (in Corps) mgenerator2Tr1: $\llbracket 0 < n; j \leq n; k \leq n; distinct-pds K n P \rrbracket \implies$
 $(\nu_K (P j)) (mprod-exp K (\lambda l. \gamma_k l) (Kb_{K n P} n)) = (\gamma_k j) *_a (\delta_j j)$
 ⟨proof⟩

lemma (in Corps) mgenerator2Tr2: $\llbracket 0 < n; j \leq n; k \leq n; distinct-pds K n P \rrbracket \implies$
 $(\nu_K (P j)) ((mprod-exp K (\lambda l. \gamma_k l) (Kb_{K n P} n))_{K^m}) = ant (m * (\gamma_k j))$
 ⟨proof⟩

lemma (in Corps) mgenerator2Tr3-1: $\llbracket 0 < n; j \leq n; k \leq n; j = k; distinct-pds K n P \rrbracket \implies$
 $(\nu_K (P j)) ((mprod-exp K (\lambda l. (\gamma_k l)) (Kb_{K n P} n))_{K^m}) = 0$
 ⟨proof⟩

lemma (in Corps) mgenerator2Tr3-2: $\llbracket 0 < n; j \leq n; k \leq n; j \neq k; distinct-pds K n P \rrbracket \implies$
 $(\nu_K (P j)) ((mprod-exp K (\lambda l. (\gamma_k l)) (Kb_{K n P} n))_{K^m}) = ant m$
 ⟨proof⟩

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

definition
 m-zmax-pdsI-hom :: $[-, nat \Rightarrow ('b \Rightarrow ant) set, 'b set] \Rightarrow nat \Rightarrow int$ **where**
 m-zmax-pdsI-hom K P I = $(\lambda j. tna (AMin ((\nu_K (P j)) 'I))$

definition
 m-zmax-pdsI :: $[-, nat, nat \Rightarrow ('b \Rightarrow ant) set, 'b set] \Rightarrow int$ **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: $\llbracket 0 < n; distinct-pds K n P; ideal (O_{K P n}) I; I \neq \{0_{O_{K P n}}\}; I \neq carrier (O_{K P n}); j \leq n; l \leq n \rrbracket \implies$
 $0 \leq ((\nu_K (P j)) (Zl-mI K P I l))$
 ⟨proof⟩

lemma (in Corps) *value-mI-genTr1*: $\llbracket 0 < n; \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I;$
 $I \neq \{\mathbf{0}_{O_{K \ P \ n}}\}; I \neq \text{carrier } (O_{K \ P \ n}); j \leq n \rrbracket \implies$
 $(\text{mprod-exp } K \ (K\text{-gamma } j) \ (Kb_{K \ n \ P}) \ n)_K^{(m\text{-zmax-pdsI } K \ n \ P \ I)} \in \text{carrier } K$
<proof>

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

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

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

lemma (in Corps) *value-mI-gen*: $\llbracket 0 < n; \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I;$
 $I \neq \{\mathbf{0}_{(O_{K \ P \ n})}\}; I \neq \text{carrier } (O_{K \ P \ n}); j \leq n \rrbracket \implies$
 $(\nu_K \ (P \ j)) \ (n\text{sum } K \ (\lambda k. ((Zl\text{-mI } K \ P \ I \ k) \cdot_r ((\text{mprod-exp } K \ (\lambda l. (\gamma_k \ l)) \ (Kb_{K \ n \ P}) \ n)_K^{(m\text{-zmax-pdsI } K \ n \ P \ I)})))) \ n) = LI \ K \ (\nu_K \ (P \ j)) \ I$
<proof>

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

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

definition

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

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

lemma (in Corps) value-mI-gen1: $\llbracket 0 < n; \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I; I \neq \{\mathbf{0}_{(O_{K \ P \ n})}\}; I \neq \text{carrier } (O_{K \ P \ n}) \rrbracket \implies$
 $\forall j \leq n. (\nu_K \ (P \ j)) \ (mIg_{K \ n \ P \ I}) = LI \ K \ (\nu_K \ (P \ j)) \ I$
 ⟨proof⟩

lemma (in Corps) mI-gen-in-I1: $\llbracket 0 < n; \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I; I \neq \{\mathbf{0}_{(O_{K \ P \ n})}\}; I \neq \text{carrier } (O_{K \ P \ n}) \rrbracket \implies (mIg_{K \ n \ P \ I}) \in I$
 ⟨proof⟩

lemma (in Corps) mI-principalTr: $\llbracket 0 < n; \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I; I \neq \{\mathbf{0}_{(O_{K \ P \ n})}\}; I \neq \text{carrier } (O_{K \ P \ n}); x \in I \rrbracket \implies$
 $\forall j \leq n. ((\nu_K \ (P \ j)) \ (mIg_{K \ n \ P \ I})) \leq ((\nu_K \ (P \ j)) \ x)$
 ⟨proof⟩

lemma (in Corps) mI-principal: $\llbracket 0 < n; \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I; I \neq \{\mathbf{0}_{(O_{K \ P \ n})}\}; I \neq \text{carrier } (O_{K \ P \ n}) \rrbracket \implies$
 $I = Rxa \ (O_{K \ P \ n}) \ (mIg_{K \ n \ P \ I})$
 ⟨proof⟩

2.8.2 prime-n-pd

lemma (in Corps) prime-n-pd-principal: $\llbracket \text{distinct-pds } K \ n \ P; j \leq n \rrbracket \implies$
 $(P_{K \ P \ n \ j}) = Rxa \ (O_{K \ P \ n}) \ (((Kb_{K \ n \ P}) \ j))$
 ⟨proof⟩

lemma (in Corps) ring-n-prod-primesTr: $\llbracket 0 < n; \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I; I \neq \{\mathbf{0}_{O_{K \ P \ n}}\}; I \neq \text{carrier } (O_{K \ P \ n}) \rrbracket \implies$
 $\forall j \leq n. (\nu_K \ (P \ j)) \ (mprod\text{-exp } K \ (mL \ K \ P \ I) \ (Kb_{K \ n \ P}) \ n) =$
 $(\nu_K \ (P \ j)) \ (mIg_{K \ n \ P \ I})$
 ⟨proof⟩

lemma (in Corps) ring-n-prod-primesTr1: $\llbracket 0 < n; \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I; I \neq \{\mathbf{0}_{O_{K \ P \ n}}\}; I \neq \text{carrier } (O_{K \ P \ n}) \rrbracket \implies$
 $I = (O_{K \ P \ n}) \ \diamond_p \ (mprod\text{-exp } K \ (mL \ K \ P \ I) \ (Kb_{K \ n \ P}) \ n)$
 ⟨proof⟩

lemma (in Corps) ring-n-prod-primes: $\llbracket 0 < n; \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I; I \neq \{\mathbf{0}_{O_{K \ P \ n}}\}; I \neq \text{carrier } (O_{K \ P \ n});$
 $\forall k \leq n. J \ k = (P_{K \ P \ n \ k}) \ \diamond^{(O_{K \ P \ n})} \ (\text{nat } ((mL \ K \ P \ I) \ k)) \rrbracket \implies$
 $I = i\Pi_{(O_{K \ P \ n}), n} \ J$
 ⟨proof⟩

end

theory Valuation3
imports Valuation2

begin

2.9 Completion

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

definition

$$\begin{aligned} \text{limit} &:: [-, 'b \Rightarrow \text{ant}, \text{nat} \Rightarrow 'b, 'b] \\ &\Rightarrow \text{bool} ((\lambda \text{lim} _ _ _ _ [90,90,90,91]90) \text{ where} \\ \text{lim}_{K v} f b &\longleftrightarrow (\forall N. \exists M. (\forall n. M < n \longrightarrow \\ &((f n) \pm_K (-_a b)) \in (\text{vp } K v) (\text{Vr } K v) (\text{an } N)))) \end{aligned}$$

lemma *not-in-singleton-noneq*: $x \notin \{a\} \implies x \neq a$
 <proof>

lemma *noneq-not-in-singleton*: $x \neq a \implies x \notin \{a\}$
 <proof>

lemma *inf-neq-1*[simp]: $\infty \neq 1$
 <proof>

lemma *a1-neq-0*[simp]: $(1::\text{ant}) \neq 0$
 <proof>

lemma *a1-poss*[simp]: $(0::\text{ant}) < 1$
 <proof>

lemma *a-p1-gt*[simp]: $\llbracket a \neq \infty; a \neq -\infty \rrbracket \implies a < a + 1$
 <proof>

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

lemma (in *Corps*) *limit-diff-n-val*: $\llbracket b \in \text{carrier } K; \forall j. f j \in \text{carrier } K;$
 $\text{valuation } K v \rrbracket \implies (\text{lim}_{K v} f b) = (\forall N. \exists M. \forall n. M < n \longrightarrow$
 $(\text{an } N) \leq (\text{n-val } K v ((f n) \pm (-_a b))))$
 <proof>

lemma (in *Corps*) *an-na-Lv*: $\text{valuation } K v \implies \text{an } (\text{na } (\text{Lv } K v)) = \text{Lv } K v$
 <proof>

lemma (in *Corps*) *limit-diff-val*: $\llbracket b \in \text{carrier } K; \forall j. f j \in \text{carrier } K;$
 $\text{valuation } K v \rrbracket \implies (\text{lim}_{K v} f b) = (\forall N. \exists M. \forall n. M < n \longrightarrow$
 $(\text{an } N) \leq (v ((f n) \pm (-_a b))))$
 <proof>

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

lemma (in *Corps*) *limit-unique*: $\llbracket b \in \text{carrier } K; \forall j. f j \in \text{carrier } K;$
 $\text{valuation } K v; c \in \text{carrier } K; \lim_{K v} f b; \lim_{K v} f c \rrbracket \implies b = c$
 <proof>

lemma (in *Corps*) *limit-n-val*: $\llbracket b \in \text{carrier } K; b \neq \mathbf{0}; \text{valuation } K v;$
 $\forall j. f j \in \text{carrier } K; \lim_{K v} f b \rrbracket \implies$
 $\exists N. (\forall m. N < m \longrightarrow (n\text{-val } K v) (f m) = (n\text{-val } K v) b)$
 <proof>

lemma (in *Corps*) *limit-val*: $\llbracket b \in \text{carrier } K; b \neq \mathbf{0}; \forall j. f j \in \text{carrier } K;$
 $\text{valuation } K v; \lim_{K v} f b \rrbracket \implies \exists N. (\forall n. N < n \longrightarrow v (f n) = v b)$
 <proof>

lemma (in *Corps*) *limit-val-infinity*: $\llbracket \text{valuation } K v; \forall j. f j \in \text{carrier } K;$
 $\lim_{K v} f \mathbf{0} \rrbracket \implies \forall N. (\exists M. (\forall m. M < m \longrightarrow (an N) \leq (n\text{-val } K v (f m))))$
 <proof>

lemma (in *Corps*) *not-limit-zero*: $\llbracket \text{valuation } K v; \forall j. f j \in \text{carrier } K;$
 $\neg (\lim_{K v} f \mathbf{0}) \rrbracket \implies \exists N. (\forall M. (\exists m. (M < m) \wedge$
 $((n\text{-val } K v) (f m)) < (an N)))$
 <proof>

lemma (in *Corps*) *limit-p*: $\llbracket \text{valuation } K v; \forall j. f j \in \text{carrier } K;$
 $\forall j. g j \in \text{carrier } K; b \in \text{carrier } K; c \in \text{carrier } K; \lim_{K v} f b; \lim_{K v} g c \rrbracket$
 $\implies \lim_{K v} (\lambda j. (f j) \pm (g j)) (b \pm c)$
 <proof>

lemma (in *Corps*) *Abs-ant-abs[simp]*: $\text{Abs } (ant z) = ant (abs z)$
 <proof>

lemma (in *Corps*) *limit-t-nonzero*: $\llbracket \text{valuation } K v; \forall (j::nat). (f j) \in \text{carrier } K;$
 $\forall (j::nat). g j \in \text{carrier } K; b \in \text{carrier } K; c \in \text{carrier } K; b \neq \mathbf{0}; c \neq \mathbf{0};$
 $\lim_{K v} f b; \lim_{K v} g c \rrbracket \implies \lim_{K v} (\lambda j. (f j) \cdot_r (g j)) (b \cdot_r c)$
 <proof>

lemma *an-npn[simp]*: $an (n + m) = an n + an m$
 <proof>

lemma *Abs-noninf*: $a \neq -\infty \wedge a \neq \infty \implies Abs a \neq \infty$
 <proof>

lemma (in *Corps*) *limit-t-zero*: $\llbracket c \in \text{carrier } K; \text{valuation } K v;$
 $\forall (j::nat). f j \in \text{carrier } K; \forall (j::nat). g j \in \text{carrier } K;$
 $\lim_{K v} f \mathbf{0}; \lim_{K v} g c \rrbracket \implies \lim_{K v} (\lambda j. (f j) \cdot_r (g j)) \mathbf{0}$
 <proof>

lemma (in *Corps*) *limit-minus*: $\llbracket \text{valuation } K \ v; \forall j. f \ j \in \text{carrier } K; b \in \text{carrier } K; \lim_{K \ v} f \ b \rrbracket \implies \lim_{K \ v} (\lambda j. (-_a (f \ j))) (-_a \ b)$
 ⟨proof⟩

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

lemma *times2plus*: $(2::\text{nat}) * n = n + n$
 ⟨proof⟩

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

definition

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

definition

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

lemma (in *Corps*) *has-limit-Cauchy*: $\llbracket \text{valuation } K \ v; \forall j. f \ j \in \text{carrier } K; b \in \text{carrier } K; \lim_{K \ v} f \ b \rrbracket \implies \text{Cauchy}_{K \ v} f$
 ⟨proof⟩

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

lemma (in *Corps*) *no-limit-zero-Cauchy1*: $\llbracket \text{valuation } K \ v; \forall j. f \ j \in \text{carrier } K; \text{Cauchy}_{K \ v} f; \neg (\lim_{K \ v} f \ \mathbf{0}) \rrbracket \implies \exists N \ M. (\forall m. N < m \longrightarrow v (f \ M) = v (f \ m))$
 ⟨proof⟩

definition

subfield :: $[-, ('b, 'm1) \text{Ring-scheme}] \Rightarrow \text{bool}$ **where**
subfield $K \ K' \longleftrightarrow \text{Corps } K' \wedge \text{carrier } K \subseteq \text{carrier } K' \wedge \text{idmap} (\text{carrier } K) \in r\text{Hom } K \ K'$

definition

v -completion $:: [!b \Rightarrow \text{ant}, !b \Rightarrow \text{ant}, -, (!b, !m) \text{ Ring-scheme}] \Rightarrow \text{bool}$
 $((\text{Completion} \text{ - - - } [90,90,90,91]90) \text{ where}$
 $\text{Completion}_{v v'} K K' \longleftrightarrow \text{subfield } K K' \wedge$
 $\text{Complete}_{v v'} K' \wedge (\forall x \in \text{carrier } K. v x = v' x) \wedge$
 $(\forall x \in \text{carrier } K'. (\exists f. \text{Cauchy}_{K v} f \wedge \lim_{K' v'} f x))$

lemma (in Corps) $\text{subfield-zero}::[\text{Corps } K'; \text{subfield } K K'] \Longrightarrow \mathbf{0}_K = \mathbf{0}_{K'}$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{subfield-pOp}::[\text{Corps } K'; \text{subfield } K K'; x \in \text{carrier } K;$
 $y \in \text{carrier } K'] \Longrightarrow x \pm y = x \pm_{K'} y$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{subfield-mOp}::[\text{Corps } K'; \text{subfield } K K'; x \in \text{carrier } K] \Longrightarrow$
 $-_a x = -_a_{K'} x$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{completion-val-eq}::[\text{Corps } K'; \text{valuation } K v; \text{valuation } K' v';$
 $x \in \text{carrier } K; \text{Completion}_{v v'} K K'] \Longrightarrow v x = v' x$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{completion-subset}::[\text{Corps } K'; \text{valuation } K v; \text{valuation } K' v';$
 $\text{Completion}_{v v'} K K'] \Longrightarrow \text{carrier } K \subseteq \text{carrier } K'$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{completion-subfield}::[\text{Corps } K'; \text{valuation } K v;$
 $\text{valuation } K' v'; \text{Completion}_{v v'} K K'] \Longrightarrow \text{subfield } K K'$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{subfield-sub}::\text{subfield } K K' \Longrightarrow \text{carrier } K \subseteq \text{carrier } K'$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{completion-Vring-sub}::[\text{Corps } K'; \text{valuation } K v;$
 $\text{valuation } K' v'; \text{Completion}_{v v'} K K'] \Longrightarrow$
 $\text{carrier } (\text{Vr } K v) \subseteq \text{carrier } (\text{Vr } K' v')$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{completion-idmap-rHom}::[\text{Corps } K'; \text{valuation } K v;$
 $\text{valuation } K' v'; \text{Completion}_{v v'} K K'] \Longrightarrow$
 $I_{(\text{Vr } K v)} \in \text{rHom } (\text{Vr } K v) (\text{Vr } K' v')$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{completion-vpr-sub}::[\text{Corps } K'; \text{valuation } K v; \text{valuation } K' v';$
 $\text{Completion}_{v v'} K K'] \Longrightarrow \text{vp } K v \subseteq \text{vp } K' v'$
 $\langle \text{proof} \rangle$

lemma (in Corps) $\text{val-v-completion}::[\text{Corps } K'; \text{valuation } K v; \text{valuation } K' v';$
 $x \in \text{carrier } K'; x \neq \mathbf{0}_{K'}; \text{Completion}_{v v'} K K'] \Longrightarrow$
 $\exists f. (\text{Cauchy}_{K v} f) \wedge (\exists N. (\forall m. N < m \longrightarrow v (f m) = v' x))$

$\langle \text{proof} \rangle$

lemma (in Corps) *v-completion-v-limit*: $\llbracket \text{Corps } K'; \text{ valuation } K v;$
 $x \in \text{carrier } K; \text{ subfield } K K'; \text{ Complete}_{v'} K'; \forall j. f j \in \text{carrier } K;$
 $\text{valuation } K' v'; \forall x \in \text{carrier } K. v x = v' x; \lim_{K' v'} f x \rrbracket \implies \lim_{K v} f x$
 $\langle \text{proof} \rangle$

lemma (in Corps) *Vr-idmap-aHom*: $\llbracket \text{Corps } K'; \text{ valuation } K v; \text{ valuation } K' v';$
 $\text{subfield } K K'; \forall x \in \text{carrier } K. v x = v' x \rrbracket \implies$
 $I_{(Vr K v)} \in \text{aHom } (Vr K v) (Vr K' v')$
 $\langle \text{proof} \rangle$

lemma *amult-pos-pos*: $0 \leq a \implies 0 \leq a * a n N$
 $\langle \text{proof} \rangle$

lemma (in Corps) *Cauchy-down*: $\llbracket \text{Corps } K'; \text{ valuation } K v; \text{ valuation } K' v';$
 $\text{subfield } K K'; \forall x \in \text{carrier } K. v x = v' x; \forall j. f j \in \text{carrier } K; \text{ Cauchy}_{K' v'} f \rrbracket$
 $\implies \text{Cauchy}_{K v} f$
 $\langle \text{proof} \rangle$

lemma (in Corps) *Cauchy-up*: $\llbracket \text{Corps } K'; \text{ valuation } K v; \text{ valuation } K' v';$
 $\text{Completion}_{v'} K K'; \text{ Cauchy}_{K v} f \rrbracket \implies \text{Cauchy}_{K' v'} f$
 $\langle \text{proof} \rangle$

lemma *max-gtTr*: $(n::\text{nat}) < \text{max } (\text{Suc } n) (\text{Suc } m) \wedge m < \text{max } (\text{Suc } n) (\text{Suc } m)$
 $\langle \text{proof} \rangle$

lemma (in Corps) *completion-approx*: $\llbracket \text{Corps } K'; \text{ valuation } K v; \text{ valuation } K' v';$
 $\text{Completion}_{v'} K K'; x \in \text{carrier } (Vr K' v') \rrbracket \implies$
 $\exists y \in \text{carrier } (Vr K v). (y \pm_{K'} -_a K' x) \in (vp K' v')$
 $\langle \text{proof} \rangle$

lemma (in Corps) *res-v-completion-surj*: $\llbracket \text{Corps } K'; \text{ valuation } K v;$
 $\text{valuation } K' v'; \text{ Completion}_{v'} K K' \rrbracket \implies$
 $\text{surjec}_{(Vr K v), (\text{gring } (Vr K' v') (vp K' v'))}$
 $(\text{compos } (Vr K v) (\text{pj } (Vr K' v') (vp K' v')) (I_{(Vr K v)}))$
 $\langle \text{proof} \rangle$

lemma (in Corps) *res-v-completion-ker*: $\llbracket \text{Corps } K'; \text{ valuation } K v;$
 $\text{valuation } K' v'; \text{ Completion}_{v'} K K' \rrbracket \implies$
 $\text{ker}_{(Vr K v), (\text{gring } (Vr K' v') (vp K' v'))}$
 $(\text{compos } (Vr K v) (\text{pj } (Vr K' v') (vp K' v')) (I_{(Vr K v)})) = vp K v$
 $\langle \text{proof} \rangle$

lemma (in Corps) *completion-res-gring-isom*: $\llbracket \text{Corps } K'; \text{ valuation } K v;$
 $\text{valuation } K' v'; \text{ Completion}_{v'} K K' \rrbracket \implies$
 $r\text{-isom } ((Vr K v) /_r (vp K v)) ((Vr K' v') /_r (vp K' v'))$

<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

$Kxa :: [-, 'b \Rightarrow ant, 'b] \Rightarrow 'b$ set **where**
 $Kxa K v x = \{y. \exists k \in carrier (Vr K v). y = x \cdot_r K k\}$

primrec

$partial-sum :: [('b, 'm) Ring-scheme, 'b, 'b \Rightarrow ant, 'b] \Rightarrow nat \Rightarrow 'b$
 $((5psum - - - -) [96,96,96,96,97]96)$

where

$psum-0: psum K x v t 0 = (csrp-fn (Vr K v) (vp K v) (pj (Vr K v) (vp K v) (x \cdot_r K t_K^{- (tna (v x))}))) \cdot_r K (t_K^{tna (v x)})$
 $| psum-Suc: psum K x v t (Suc n) = (psum K x v t n) \pm_K ((csrp-fn (Vr K v) (vp K v) (pj (Vr K v) (vp K v) ((x \pm_K -_a K (psum K x v t n)) \cdot_r K (t_K^{- (tna (v x) + int (Suc n))})))) \cdot_r K (t_K^{tna (v x) + int (Suc n)}))$

definition

$expand-coeff :: [-, 'b \Rightarrow ant, 'b, 'b] \Rightarrow nat \Rightarrow 'b$
 $((5ecf - - - -) [96,96,96,96,97]96)$ **where**
 $ecf K v t x n = (if n = 0 then csrp-fn (Vr K v) (vp K v) (pj (Vr K v) (vp K v) (x \cdot_r K t_K^{- (tna (v x))})))$
 $else csrp-fn (Vr K v) (vp K v) (pj (Vr K v) (vp K v) ((x \pm_K -_a K (psum K x v t (n - 1))) \cdot_r K (t_K^{- (tna (v x) + int n))}))))$

definition

$expand-term :: [-, 'b \Rightarrow ant, 'b, 'b] \Rightarrow nat \Rightarrow 'b$
 $((5etm - - - -) [96,96,96,96,97]96)$ **where**

$etm K v t x n = (ecf K v t x n) \cdot_r K (t_K^{tna (v x) + int n})$

lemma (in Corps) $Kxa-val-ge$: $\llbracket valuation K v; t \in carrier K; v t = 1 \rrbracket$

$\implies Kxa K v (t_K^j) = \{x. x \in carrier K \wedge (ant j) \leq (v x)\}$

<proof>

lemma (in Corps) $Kxa-pow-vpr$: $\llbracket valuation K v; t \in carrier K; v t = 1; (0::int) \leq j \rrbracket \implies Kxa K v (t_K^j) = (vp K v)(Vr K v) (ant j)$

<proof>

lemma (in Corps) *field-distribTr*: $\llbracket a \in \text{carrier } K; b \in \text{carrier } K; x \in \text{carrier } K; x \neq \mathbf{0} \rrbracket \implies a \pm (-_a (b \cdot_r x)) = (a \cdot_r (x^{-K}) \pm (-_a b)) \cdot_r x$
<proof>

lemma *a0-le-1[simp]*: $(0::\text{int}) \leq 1$
<proof>

lemma (in Corps) *vp-mem-times-t*: $\llbracket \text{valuation } K v; t \in \text{carrier } K; t \neq \mathbf{0}; v t = 1; x \in \text{vp } K v \rrbracket \implies \exists a \in \text{carrier } (Vr K v). x = a \cdot_r t$
<proof>

lemma (in Corps) *psum-diff-mem-Kxa*: $\llbracket \text{valuation } K v; t \in \text{carrier } K; v t = 1; x \in \text{carrier } K; x \neq \mathbf{0} \rrbracket \implies$
 $(\text{psum } K x v t n) \in \text{carrier } K \wedge$
 $(x \pm (-_a (\text{psum } K x v t n))) \in Kxa K v (t_K^{((tna (v x)) + (1 + \text{int } n))})$
<proof>

lemma *Suc-diff-int*: $0 < n \implies \text{int } (n - \text{Suc } 0) = \text{int } n - 1$
<proof>

lemma (in Corps) *ecf-mem*: $\llbracket \text{valuation } K v; t \in \text{carrier } K; v t = 1; x \in \text{carrier } K; x \neq \mathbf{0} \rrbracket \implies \text{ecf}_{K v t x} n \in \text{carrier } K$
<proof>

lemma (in Corps) *etm-mem*: $\llbracket \text{valuation } K v; t \in \text{carrier } K; v t = 1; x \in \text{carrier } K; x \neq \mathbf{0} \rrbracket \implies \text{etm}_{K v t x} n \in \text{carrier } K$
<proof>

lemma (in Corps) *psum-sum-etm*: $\llbracket \text{valuation } K v; t \in \text{carrier } K; v t = 1; x \in \text{carrier } K; x \neq \mathbf{0} \rrbracket \implies$
 $\text{psum}_{K x v t} n = \text{nsum } K (\lambda j. (\text{ecf}_{K v t x} j) \cdot_r (t_K^{(tna (v x) + (\text{int } j))})) n$
<proof>

lemma *zabs-pos*: $0 \leq (\text{abs } (z::\text{int}))$
<proof>

lemma *abs-p-self-pos*: $0 \leq z + (\text{abs } (z::\text{int}))$
<proof>

lemma *zadd-right-mono*: $(i::\text{int}) \leq j \implies i + k \leq j + k$
<proof>

theorem (in Corps) *expansion-thm*: $\llbracket \text{valuation } K v; t \in \text{carrier } K; v t = 1; x \in \text{carrier } K; x \neq \mathbf{0} \rrbracket \implies \lim_{K v} (\text{partial-sum } K x v t) x$
<proof>

2.9.1 Hensel's theorem

definition

pol-Cauchy-seq :: [(*'b*, *'m*) Ring-scheme, *'b*, -, *'b* ⇒ *ant*,
nat ⇒ *'b*] ⇒ *bool* ((5*PCauchy* - - - -) [90,90,90,90,91]90) **where**
*PCauchy*_{*R*} *X* *K* *v* *F* ⇔ (∀ *n*. (*F n*) ∈ *carrier R*) ∧
(∃ *d*. (∀ *n*. *deg R* (Vr *K v*) *X* (*F n*) ≤ (*an 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*))))

definition

pol-limit :: [(*'b*, *'m*) Ring-scheme, *'b*, -, *'b* ⇒ *ant*,
nat ⇒ *'b*, *'b*] ⇒ *bool*
((6*Plimit* - - - -) [90,90,90,90,90,91]90) **where**
*Plimit*_{*R*} *X* *K* *v* *F* *p* ⇔ (∀ *n*. (*F n*) ∈ *carrier R*) ∧
(∀ *N*. ∃ *M*. (∀ *m*. *M* < *m* →
P-mod R (Vr *K v*) *X* ((*vp K v*)^(Vr *K v*) (*an N*)) ((*F m*) ±_{*R*} -_{*a*}*R* (*p*)))

definition

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

definition

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

lemma *an-neq-minf[simp]*: ∀ *n*. -∞ ≠ *an n*
⟨*proof*⟩

lemma *an-neq-minf1[simp]*: ∀ *n*. *an n* ≠ -∞
⟨*proof*⟩

lemma (in *Corps*) *Pseql-mem*: [[*valuation K v*; *PolynRg R* (Vr *K v*) *X*;
F n ∈ *carrier R*; ∀ *n*. *deg R* (Vr *K v*) *X* (*F n*) ≤ *an* (*Suc d*)] ⇒
(*Pseql*_{*R*} *X* *K* *v* *d* *F*) *n* ∈ *carrier R*
⟨*proof*⟩

lemma (in *Corps*) *Pseqh-mem*: [[*valuation K v*; *PolynRg R* (Vr *K v*) *X*;
F n ∈ *carrier R*; ∀ *n*. *deg R* (Vr *K v*) *X* (*F n*) ≤ *an* (*Suc d*)] ⇒
(*Pseqh*_{*R*} *X* *K* *v* *d* *F*) *n* ∈ *carrier R*

$\langle \text{proof} \rangle$

lemma (in *Corps*) *PCauchy-lTr*: $\llbracket \text{valuation } K v; \text{PolynRg } R (Vr K v) X;$
 $p \in \text{carrier } R; \text{deg } R (Vr K v) X p \leq \text{an } (Suc d);$
 $P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v) (an N)}) p \rrbracket \implies$
 $P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v) (an N)}) (ldeg\text{-}p R (Vr K v) X d p)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *PCauchy-hTr*: $\llbracket \text{valuation } K v; \text{PolynRg } R (Vr K v) X;$
 $p \in \text{carrier } R; \text{deg } R (Vr K v) X p \leq \text{an } (Suc d);$
 $P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v) (an N)}) p \rrbracket$
 $\implies P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v) (an N)}) (hdeg\text{-}p R (Vr K v) X (Suc$
 $d) p)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *v-ldeg-p-pOp*: $\llbracket \text{valuation } K v; \text{PolynRg } R (Vr K v) X;$
 $p \in \text{carrier } R; q \in \text{carrier } R; \text{deg } R (Vr K v) X p \leq \text{an } (Suc d);$
 $\text{deg } R (Vr K v) X q \leq \text{an } (Suc d) \rrbracket \implies$
 $(ldeg\text{-}p R (Vr K v) X d p) \pm_R (ldeg\text{-}p R (Vr K v) X d q) =$
 $ldeg\text{-}p R (Vr K v) X d (p \pm_R q)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *v-hdeg-p-pOp*: $\llbracket \text{valuation } K v; \text{PolynRg } R (Vr K v) X;$
 $p \in \text{carrier } R; q \in \text{carrier } R; \text{deg } R (Vr K v) X p \leq \text{an } (Suc d);$
 $\text{deg } R (Vr K v) X q \leq \text{an } (Suc d) \rrbracket \implies (hdeg\text{-}p R (Vr K v) X (Suc d) p) \pm_R$
 $(hdeg\text{-}p R (Vr K v) X (Suc d) q) = hdeg\text{-}p R (Vr K v) X (Suc d) (p \pm_R q)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *v-ldeg-p-mOp*: $\llbracket \text{valuation } K v; \text{PolynRg } R (Vr K v) X;$
 $p \in \text{carrier } R; \text{deg } R (Vr K v) X p \leq \text{an } (Suc d) \rrbracket \implies$
 $-_a R (ldeg\text{-}p R (Vr K v) X d p) = ldeg\text{-}p R (Vr K v) X d (-_a R p)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *v-hdeg-p-mOp*: $\llbracket \text{valuation } K v; \text{PolynRg } R (Vr K v) X;$
 $p \in \text{carrier } R; \text{deg } R (Vr K v) X p \leq \text{an } (Suc d) \rrbracket \implies$
 $-_a R (hdeg\text{-}p R (Vr K v) X (Suc d) p) = hdeg\text{-}p R (Vr K v) X (Suc d) (-_a R$
 $p)$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *PCauchy-lPCauchy*: $\llbracket \text{valuation } K v; \text{PolynRg } R (Vr K v) X;$
 $\forall n. F n \in \text{carrier } R; \forall n. \text{deg } R (Vr K v) X (F n) \leq \text{an } (Suc d);$
 $P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v) (an N)}) (F n \pm_R -_a R (F m)) \rrbracket$
 $\implies P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v) (an N)})$
 $((Pseq1_R X K v d F) n) \pm_R -_a R ((Pseq1_R X K v d F) m))$
 $\langle \text{proof} \rangle$

lemma (in *Corps*) *PCauchy-hPCauchy*: $\llbracket \text{valuation } K v; \text{PolynRg } R (Vr K v) X;$

$\forall n. F n \in \text{carrier } R; \forall n. \text{deg } R (Vr K v) X (F n) \leq an (Suc d);$
 $P\text{-mod } R (Vr K v) X (vp K v (Vr K v) (an N)) (F n \pm_R -aR (F m))$
 $\implies P\text{-mod } R (Vr K v) X (vp K v (Vr K v) (an N))$
 $((Pseqh_R X K v d F) n) \pm_R -aR ((Pseqh_R X K v d F) m)$
 <proof>

lemma (in Corps) Pseq-decompos:[[valuation K v; PolynRg R (Vr K v) X;
 $F n \in \text{carrier } R; \text{deg } R (Vr K v) X (F n) \leq an (Suc d)$]]
 $\implies F n = ((Pseql_R X K v d F) n) \pm_R ((Pseqh_R X K v d F) n)$
 <proof>

lemma (in Corps) deg-0-const:[[valuation K v; PolynRg R (Vr K v) X;
 $p \in \text{carrier } R; \text{deg } R (Vr K v) X p \leq 0$]] $\implies p \in \text{carrier } (Vr K v)$
 <proof>

lemma (in Corps) monomial-P-limit:[[valuation K v; Complete_v K;
 PolynRg R (Vr K v) X; $\forall n. f n \in \text{carrier } (Vr K v);$
 $\forall n. F n = (f n) \cdot_{rR} (X^{^R} d); \forall N. \exists M. \forall n m. M < n \wedge M < m \longrightarrow$
 $P\text{-mod } R (Vr K v) X (vp K v (Vr K v) (an N)) (F n \pm_R -aR (F m))$]] \implies
 $\exists b \in \text{carrier } (Vr K v). Plimit_R X K v F (b \cdot_{rR} (X^{^R} d))$
 <proof>

lemma (in Corps) mPlimit-uniqueTr:[[valuation K v;
 PolynRg R (Vr K v) X; $\forall n. f n \in \text{carrier } (Vr K v);$
 $\forall n. F n = (f n) \cdot_{rR} (X^{^R} d); c \in \text{carrier } (Vr K v);$
 $Plimit_R X K v F (c \cdot_{rR} (X^{^R} d))$]] $\implies \lim K v f c$
 <proof>

lemma (in Corps) mono-P-limit-unique:[[valuation K v;
 PolynRg R (Vr K v) X; $\forall n. f n \in \text{carrier } (Vr K v);$
 $\forall n. F n = (f n) \cdot_{rR} (X^{^R} d); b \in \text{carrier } (Vr K v); c \in \text{carrier } (Vr K v);$
 $Plimit_R X K v F (b \cdot_{rR} (X^{^R} d)); Plimit_R X K v F (c \cdot_{rR} (X^{^R} d))$]] \implies
 $b \cdot_{rR} (X^{^R} d) = c \cdot_{rR} (X^{^R} d)$
 <proof>

lemma (in Corps) Plimit-deg:[[valuation K v; PolynRg R (Vr K v) X;
 $\forall n. F n \in \text{carrier } R; \forall n. \text{deg } R (Vr K v) X (F n) \leq (an d);$
 $p \in \text{carrier } R; Plimit_R X K v F p$]] $\implies \text{deg } R (Vr K v) X p \leq (an d)$
 <proof>

lemma (in Corps) Plimit-deg1:[[valuation K v; Ring R; PolynRg R (Vr K v) X;
 $\forall n. F n \in \text{carrier } R; \forall n. \text{deg } R (Vr K v) X (F n) \leq ad;$
 $p \in \text{carrier } R; Plimit_R X K v F p$]] $\implies \text{deg } R (Vr K v) X p \leq ad$
 <proof>

lemma (in Corps) Plimit-ldeg:[[valuation K v; PolynRg R (Vr K v) X;

definition

$Hsnd :: [-, 'b \Rightarrow ant, ('b, 'm1) \text{ Ring-scheme}, 'b, 'b, ('b \text{ set}, 'm2) \text{ Ring-scheme}, 'b \text{ set}, 'b, 'b, 'b, nat] \Rightarrow 'b$

$((11Hsnd \text{ ----- } -) [67,67,67,67,67,67,67,67,67,67,68]67) \text{ where}$

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

lemma (in Corps) Hensel-starter: \llbracket valuation $K v$; Complete $_v K$;

PolynRg $R (Vr K v) X$; PolynRg $S ((Vr K v) /_r (vp K v)) Y$;

$t \in carrier (Vr K v)$; $vp K v = (Vr K v) \diamond_p t$;

$f \in carrier R$; $f \neq \mathbf{0}_R$; $g' \in carrier S$; $h' \in carrier S$;

$0 < deg S ((Vr K v) /_r (vp K v)) Y g'$;

$0 < deg S ((Vr K v) /_r (vp K v)) Y h'$;

$((erH R (Vr K v) X S ((Vr K v) /_r (vp K v)) Y$

$(pj (Vr K v) (vp K v))) f = g' \cdot_r S h'$;

rel-prime-pols $S ((Vr K v) /_r (vp K v)) Y g' h'$ $\rrbracket \implies$

$\exists g h. g \neq \mathbf{0}_R \wedge h \neq \mathbf{0}_R \wedge g \in carrier R \wedge h \in carrier R \wedge$

$deg R (Vr K v) X g \leq deg S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$

$(erH R (Vr K v) X S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$

$(pj (Vr K v) ((Vr K v) \diamond_p t)) g) \wedge (deg R (Vr K v) X h +$

$deg S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y (erH R (Vr K v) X S$

$((Vr K v) /_r ((Vr K v) \diamond_p t)) Y (pj (Vr K v) ((Vr K v) \diamond_p t)) g)$

$\leq deg R (Vr K v) X f) \wedge$

$(erH R (Vr K v) X S ((Vr K v) /_r (vp K v)) Y$

$(pj (Vr K v) (vp K v))) g = g' \wedge$

$(erH R (Vr K v) X S ((Vr K v) /_r (vp K v)) Y$

$(pj (Vr K v) (vp K v))) h = h' \wedge$

$0 < deg S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$

$(erH R (Vr K v) X S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$

$(pj (Vr K v) ((Vr K v) \diamond_p t)) g) \wedge$

$0 < deg S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$

$(erH R (Vr K v) X S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$

$(pj (Vr K v) ((Vr K v) \diamond_p t)) h) \wedge$

rel-prime-pols $S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$

$(erH R (Vr K v) X S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$

$(pj (Vr K v) ((Vr K v) \diamond_p t)) g)$

$(erH R (Vr K v) X S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$

$(pj (Vr K v) ((Vr K v) \diamond_p t)) h) \wedge$

$P\text{-mod } R (Vr K v) X ((Vr K v) \diamond_p t) (f \pm_R -_a R (g \cdot_r R h))$

$\langle \text{proof} \rangle$

lemma aadd-plus-le-plus: $\llbracket a \leq (a'::ant); b \leq b' \rrbracket \implies a + b \leq a' + b'$

$\langle \text{proof} \rangle$

lemma (in Corps) Hfst-PCauchy: \llbracket valuation $K v$; Complete $_v K$;

PolynRg $R (Vr K v) X$; PolynRg $S (Vr K v /_r (Vr K v \diamond_p t)) Y$; $g0 \in carrier$

R ;

$h0 \in carrier R$; $f \in carrier R$; $f \neq \mathbf{0}_R$; $g0 \neq \mathbf{0}_R$; $h0 \neq \mathbf{0}_R$;

$$\begin{aligned}
& t \in \text{carrier } (Vr K v); \quad vp K v = Vr K v \diamond_p t; \\
& \text{deg } R (Vr K v) X g0 \leq \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X \\
& S \\
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0); \\
& \text{deg } R (Vr K v) X h0 + \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X \\
& S \\
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0) \\
& \quad \leq \text{deg } R (Vr K v) X f; \\
& 0 < \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X S \\
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0); \\
& 0 < \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X S \\
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) h0); \\
& \text{rel-prime-pols } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X S \\
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0) \\
& \quad (\text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad \quad (pj (Vr K v) (Vr K v \diamond_p t)) h0);
\end{aligned}$$

$$\begin{aligned}
& \text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (pj (Vr K v) (Vr K v \diamond_p t)) f = \\
& \quad \text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad \quad (pj (Vr K v) (Vr K v \diamond_p t)) g0 \cdot_{rS} \\
& \quad \text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad \quad (pj (Vr K v) (Vr K v \diamond_p t)) h0 \implies \\
& \text{PCauchy } R X K v \text{Hfst } K v R X t S Y f g0 h0
\end{aligned}$$

\langle proof \rangle

lemma (in Corps) Hsnd-PCauchy: \llbracket valuation $K v$; Complete $_v K$;

PolynRg $R (Vr K v) X$; PolynRg $S (Vr K v /_r (Vr K v \diamond_p t)) Y$; $g0 \in \text{carrier } R$;

$h0 \in \text{carrier } R$; $f \in \text{carrier } R$; $f \neq \mathbf{0}_R$; $g0 \neq \mathbf{0}_R$; $h0 \neq \mathbf{0}_R$;

$t \in \text{carrier } (Vr K v)$; $vp K v = Vr K v \diamond_p t$;

$\text{deg } R (Vr K v) X g0 \leq \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X$
 S

$$\begin{aligned}
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0); \\
& \text{deg } R (Vr K v) X h0 + \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X \\
& S \\
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0) \\
& \quad \leq \text{deg } R (Vr K v) X f; \\
& 0 < \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X S \\
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0); \\
& 0 < \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X S \\
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) h0); \\
& \text{rel-prime-pols } S (Vr K v /_r (Vr K v \diamond_p t)) Y (\text{erH } R (Vr K v) X S \\
& \quad (Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0) \\
& \quad (\text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad \quad (pj (Vr K v) (Vr K v \diamond_p t)) h0); \\
& \text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (pj (Vr K v) (Vr K v \diamond_p t)) f =
\end{aligned}$$

$$\begin{aligned}
& \text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (pj (Vr K v) (Vr K v \diamond_p t)) g0 \cdot_r S \\
& \text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (pj (Vr K v) (Vr K v \diamond_p t)) h0 \implies \\
& \text{PCauchy } R X K v \text{Hsnd } K v R X t S Y f g0 h0
\end{aligned}$$

\langle proof \rangle

lemma (in Corps) *H-Plimit-f*: [valuation $K v$; Complete $_v K$;

$t \in \text{carrier } (Vr K v)$; $vp K v = Vr K v \diamond_p t$;
PolynRg $R (Vr K v) X$; *PolynRg* $S (Vr K v /_r (Vr K v \diamond_p t)) Y$;
 $f \in \text{carrier } R$; $f \neq \mathbf{0}_R$; $g0 \in \text{carrier } R$; $h0 \in \text{carrier } R$; $g0 \neq \mathbf{0}_R$;
 $h0 \neq \mathbf{0}_R$;

$$\begin{aligned}
& 0 < \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (\text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad \quad (pj (Vr K v) (Vr K v \diamond_p t)) g0); \\
& 0 < \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (\text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad \quad (pj (Vr K v) (Vr K v \diamond_p t)) h0); \\
& \text{deg } R (Vr K v) X h0 + \\
& \quad \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (\text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad \quad (pj (Vr K v) (Vr K v \diamond_p t)) g0) \leq \text{deg } R (Vr K v) X f;
\end{aligned}$$

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

$$\begin{aligned}
& \text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (pj (Vr K v) (Vr K v \diamond_p t)) f = \\
& \text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (pj (Vr K v) (Vr K v \diamond_p t)) g0 \cdot_r S \\
& \text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (pj (Vr K v) (Vr K v \diamond_p t)) h0;
\end{aligned}$$

$$\begin{aligned}
& \text{deg } R (Vr K v) X g0 \\
& \leq \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad (\text{erH } R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y \\
& \quad \quad (pj (Vr K v) (Vr K v \diamond_p t)) g0);
\end{aligned}$$

$g \in \text{carrier } R$; $h \in \text{carrier } R$;

$$\begin{aligned}
& \text{Plimit } R X K v (\text{Hfst } K v R X t S Y f g0 h0) g; \\
& \text{Plimit } R X K v (\text{Hsnd } K v R X t S Y f g0 h0) h; \\
& \text{Plimit } R X K v (\lambda n. (\text{Hfst } K v R X t S Y f g0 h0 n) \cdot_r R \\
& \quad (\text{Hsnd } K v R X t S Y f g0 h0 n)) (g \cdot_r R h) \implies \\
& \text{Plimit } R X K v (\lambda n. (\text{Hfst } K v R X t S Y f g0 h0 n) \cdot_r R \\
& \quad (\text{Hsnd } K v R X t S Y f g0 h0 n)) f
\end{aligned}$$

$\langle proof \rangle$

theorem (in Corps) Hensel: $\llbracket valuation\ K\ v; Complete_v\ K;$
PolynRg $R\ (Vr\ K\ v)\ X; PolynRg\ S\ ((Vr\ K\ v)\ /_r\ (vp\ K\ v))\ Y;$
 $f \in carrier\ R; f \neq \mathbf{0}_R; g' \in carrier\ S; h' \in carrier\ S;$
 $0 < deg\ S\ ((Vr\ K\ v)\ /_r\ (vp\ K\ v))\ Y\ g';$
 $0 < deg\ S\ ((Vr\ K\ v)\ /_r\ (vp\ K\ v))\ Y\ h';$
 $((erH\ R\ (Vr\ K\ v)\ X\ S\ ((Vr\ K\ v)\ /_r\ (vp\ K\ v))\ Y$
 $\quad (pj\ (Vr\ K\ v)\ (vp\ K\ v)))\ f) = g' \cdot_{rS}\ h';$
 $rel\ prime\ polys\ S\ ((Vr\ K\ v)\ /_r\ (vp\ K\ v))\ Y\ g'\ h' \rrbracket \implies$
 $\exists g\ h. g \in carrier\ R \wedge h \in carrier\ R \wedge$
 $deg\ R\ (Vr\ K\ v)\ X\ g \leq deg\ S\ ((Vr\ K\ v)\ /_r\ (vp\ K\ v))\ Y\ g' \wedge$
 $f = g \cdot_{rR}\ h$

$\langle proof \rangle$

end