

Fundamental Properties of Valuation Theory and Hensel's Lemma

Hidetsune Kobayashi

December 7, 2022

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 vp 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	49

```
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*: $[(i::int) < j; j < k] \implies i < k$
<proof>

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

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

lemma *zless-le-trans*: $[(i::int) < j; j \leq k] \implies i < k$
<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*: $[(x::ant) \leq y; y = z] \implies x \leq z$
<proof>

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

lemma *amult-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 $K\text{delta-in-Zinf} : [j \leq (\text{Suc } n); k \leq (\text{Suc } n)] \Longrightarrow$
 $z *_a (\delta_j k) \in Z_\infty$
 $\langle \text{proof} \rangle$

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

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

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

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

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* ⇔

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

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

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

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

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

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

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 valuation K v ; $x \in$ carrier K ; $x \neq \mathbf{0}$ $\rrbracket \implies$
 $\exists z. (v\ x) = \text{ant } z$

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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*: $\llbracket \text{valuation } K v; x \in \text{carrier } K \rrbracket \implies$
 $(THE l. (l * (Lv K v)) = v x) * (Lv K v) = v x$

$\langle \text{proof} \rangle$

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

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

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

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

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

lemma (in *Corps*) *n-val-t2p*: \llbracket valuation K v ; $x \in$ carrier K ; $y \in$ 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 proof \rangle

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

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

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

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

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

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

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

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

lemma *nnonzero-annonzero*: $0 < N \implies an \ N \neq 0$
 $\langle \text{proof} \rangle$

2.3 Valuation ring

definition

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

definition

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

definition

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

abbreviation

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

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

$\langle \text{proof} \rangle$

lemma (in *Ring*) *r-apow-Suc:ideal* $R \ I \implies I^R \ (an \ (Suc \ 0)) = I$
 $\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

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

$\langle \text{proof} \rangle$

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<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*: $\llbracket \text{ideal } R I; x \in \text{carrier } R;$
 $x \notin I \rrbracket \implies x \neq \mathbf{0}_R$

<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*: $\llbracket \text{valuation } K v; 0 \leq n \rrbracket \implies$
 $\text{ideal } (Vr K v) ((vp K v) (Vr K v) n)$

<proof>

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

<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 $K v \implies$
 $\text{maximal-ideal } (Vr K v) (vp K v)$

$\langle \text{proof} \rangle$

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 $K v \implies$
 $\text{Corps } ((Vr K v) /_r (vp K v))$

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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*: $\llbracket \text{valuation } K v; 0 \leq n \rrbracket \implies$

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

2.4.1 Amin lemma (in Corps)s

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

<proof>

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

<proof>

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

<proof>

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

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

2.5 pow of vp and n -value – convergence –

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

⟨proof⟩

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

⟨proof⟩

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

⟨proof⟩

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

⟨proof⟩

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

⟨proof⟩

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

⟨proof⟩

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

⟨proof⟩

lemma (in *Corps*) vp-potent-zero :⟦valuation $K v$; $0 \leq n$ ⟧ \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: $\llbracket \text{valuation } K v; x \in \text{carrier } (Vr K v); Suc\ 0 < n \rrbracket \implies x \cdot_r (Vr K v) (x \hat{\sim}^K (n - Suc\ 0)) \in (Vr K v) \diamond_p (x \hat{\sim}^K n)$

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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*: $\llbracket valuation K v; valuation K v';$
 $carrier (Vr K v) \subseteq carrier (Vr K v') \rrbracket \implies$
 $ridmap (Vr K v) \in rHom (Vr K v) (Vr K v')$
 ⟨proof⟩

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

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

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

lemma (in Corps) *contract-maximal*: $\llbracket valuation K v; valuation K v';$
 $carrier (Vr K v) \subseteq carrier (Vr K v') \rrbracket \implies$
 $maximal-ideal (Vr K v) (carrier (Vr K v) \cap vp K v')$
 ⟨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*: $\llbracket valuation K v; valuation K v';$
 $\forall x \in carrier K. 0 \leq (v x) \longrightarrow 0 \leq (v' x) \rrbracket \implies$
 $carrier (Vr K v) \subseteq carrier (Vr K v')$
 ⟨proof⟩

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

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

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

\langle proof \rangle

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

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

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

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

\langle proof \rangle

2.7 Prime divisors

definition

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

definition

prime-divisors :: $- \Rightarrow ('b \Rightarrow \text{ant}) \text{ set set } (Pds1 \ 96) \text{ where}$
 $Pds_K = \{P. \exists v. \text{valuation } K \ v \wedge P = P_{K \ v} \}$

definition

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

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

\langle proof \rangle

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

\langle proof \rangle

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

\langle proof \rangle

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

$(\text{SOME } w. w \in P_K v) \in P_K v$
 $\langle \text{proof} \rangle$

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

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

lemma (in Corps) representative-of-pd-valuation:
 $P \in Pds \implies \text{valuation } K (\nu_K P)$
 $\langle \text{proof} \rangle$

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

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

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

lemma (in Corps) unique-n-valuation: $\llbracket P \in Pds_K; P' \in Pds \rrbracket \implies$
 $(P = P') = (\nu_K P = \nu_K P')$
 $\langle \text{proof} \rangle$

lemma (in Corps) n-val-representative: $P \in Pds \implies (\nu_K P) \in P$
 $\langle \text{proof} \rangle$

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

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

2.8 Approximation

definition

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

definition

$\text{vals-nonequiv} :: [-, \text{nat}, \text{nat} \Rightarrow ('r \Rightarrow \text{ant})] \Rightarrow \text{bool}$ **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*) $field\text{-}op\text{-}minus$: $\llbracket a \in carrier\ K; b \in carrier\ K; b \neq \mathbf{0} \rrbracket \Longrightarrow -_a\ (a \cdot_r (b^{-K})) = (-_a\ a) \cdot_r (b^{-K})$
 $\langle proof \rangle$

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

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

<proof>

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

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

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

<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-elim*: $\llbracket x \in \text{carrier } K;$

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

<proof>

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

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

<proof>

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

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

<proof>

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

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

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

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

end

theory Valuation2
imports Valuation1
begin

lemma (in Corps) OstrowskiTr8: $\llbracket \text{valuation } K \text{ } v; x \in \text{carrier } K; 0 < v \text{ (} 1_r \pm -_a x \text{)} \rrbracket \implies 0 < (v \text{ (} 1_r \pm -_a (x \cdot_r ((1_r \pm x \cdot_r (1_r \pm -_a x))^{-K}))))$
 <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*: $k \leq n \Longrightarrow \forall j \leq n. (\lambda l. \gamma_k\ l)\ j \in \text{Zset}$
 <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 vals-nonequiv K ($Suc\ n$) vv ;
 $j \leq Suc\ n \rrbracket \implies (\Omega_K\ vv\ (Suc\ n))\ j \neq \mathbf{0}$
 ⟨proof⟩

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

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

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

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

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

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

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

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

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

abbreviation

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

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

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

lemma (in Ring) *tail-of-expansion1*: $x \in \text{carrier } R \implies$
 $(1_r \pm x)^{\sim R} (\text{Suc } n) = x \cdot_r (\text{nsum } R (\lambda i. ((\text{Suc } n)C_{(\text{Suc } i)} \times_R x^{\sim R} i)) n) \pm 1_r$
 ⟨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
 $v x \leq (v (1_r \pm -_a ((1_r \pm x)^{\sim K} (\text{Suc } n))))$
 ⟨proof⟩

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

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

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

$\langle \text{proof} \rangle$

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

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

$\langle \text{proof} \rangle$

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

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

$\langle \text{proof} \rangle$

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

$$(1_r \pm -_a x) \cdot_r (n\text{sum } R (\lambda j. x^R j) n) = 1_r \pm -_a (x^R (Suc n))$$

$\langle \text{proof} \rangle$

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

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

$\langle \text{proof} \rangle$

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*: $\llbracket \text{valuation } K v; x \in \text{carrier } K;$

$$0 < (v (1_r \pm -_a x)) \rrbracket \Longrightarrow 0 < (v (1_r \pm -_a x^K (Suc n)))$$

$\langle \text{proof} \rangle$

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

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

$\langle \text{proof} \rangle$

definition

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

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

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

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

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*: $\llbracket \text{distinct-pds } K \text{ (Suc } n) \ P \rrbracket \Longrightarrow$
 $\text{distinct-pds } K \ n \ P$
 $\langle \text{proof} \rangle$

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

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

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

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

definition

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

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

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

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

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

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

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

lemma (in Corps) ring-n-eSum-K-eSum:distinct-pds $K n P;$
 $\forall j \leq m. f j \in carrier (O_{K P n}) \implies nsum (O_{K P n}) f m = nsum K f m$
 <proof>

lemma (in Corps) ideal-eSum-closed:distinct-pds $K n P; ideal (O_{K P n}) I;$
 $\forall j \leq m. f j \in I \implies nsum K f m \in I$
 <proof>

definition

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

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

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

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

$\implies x \in \text{carrier } K$
 ⟨proof⟩

lemma (in *Corps*) *ring-n-tOp-K-tOp*: $\llbracket \text{distinct-pds } K \ n \ P; x \in \text{carrier } (O_{K \ P \ n});$
 $y \in \text{carrier } (O_{K \ P \ n}) \rrbracket \implies x \cdot_r (O_{K \ P \ n}) \ y = x \cdot_r \ y$
 ⟨proof⟩

lemma (in *Corps*) *ring-n-exp-K-exp*: $\llbracket \text{distinct-pds } K \ n \ P; x \in \text{carrier } (O_{K \ P \ n}) \rrbracket$
 $\implies x \wedge^K m = x \wedge^{(O_{K \ P \ n})} m$
 ⟨proof⟩

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

lemma (in *Corps*) *n-eq-val-eq-idealTr*:
 $\llbracket \text{distinct-pds } K \ n \ P; x \in \text{carrier } (O_{K \ P \ n}); y \in \text{carrier } (O_{K \ P \ n});$
 $\forall j \leq n. ((\nu_K (P \ j)) \ x) \leq ((\nu_K (P \ j)) \ y) \rrbracket \implies \text{Rxa } (O_{K \ P \ n}) \ y \subseteq \text{Rxa } (O_{K \ P \ n}) \ x$
 ⟨proof⟩

lemma (in *Corps*) *n-eq-val-eq-ideal*: $\llbracket \text{distinct-pds } K \ n \ P; x \in \text{carrier } (O_{K \ P \ n});$
 $y \in \text{carrier } (O_{K \ P \ n}); \forall j \leq n. ((\nu_K (P \ j)) \ x) = ((\nu_K (P \ j)) \ y) \rrbracket \implies$
 $\text{Rxa } (O_{K \ P \ n}) \ x = \text{Rxa } (O_{K \ P \ n}) \ y$
 ⟨proof⟩

definition

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

definition

mL :: $[-, \text{nat} \Rightarrow ('r \Rightarrow \text{ant}) \text{ set}, 'r \text{ set}, \text{nat}] \Rightarrow \text{int}$ **where**
 $\text{mL } K \ P \ I \ j = \text{tna } (\text{LI } K \ (\nu_K (P \ j)) \ I)$

lemma (in *Corps*) *mI-vals-nonempty*: $\llbracket \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I; j \leq n \rrbracket$
 $\implies (\nu_K (P \ j)) \ 'I \neq \{\}$
 ⟨proof⟩

lemma (in *Corps*) *mI-vals-LB*: $\llbracket \text{distinct-pds } K \ n \ P; \text{ideal } (O_{K \ P \ n}) \ I; j \leq n \rrbracket \implies$
 $((\nu_K (P \ j)) \ 'I) \subseteq \text{LBset } (\text{ant } 0)$
 ⟨proof⟩

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

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

$\implies \exists x \in I. (\nu_K (P j)) x = LI K (\nu_K (P j)) I$
 ⟨proof⟩

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

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

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

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

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

$Kbase :: [-, nat, nat \Rightarrow ('r \Rightarrow ant) set] \Rightarrow (nat \Rightarrow 'r) ((\exists Kb. \dots) [95,95,96]95)$ **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-mI :: [$-, \text{nat} \Rightarrow ('b \Rightarrow \text{ant}) \text{ set}, 'b \text{ set}$]
 $\Rightarrow \text{nat} \Rightarrow 'b$ **where**

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

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

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

definition

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

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

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

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

lemma (in *Corps*) *mprod-Suc*: $\llbracket \forall j \leq (\text{Suc } n). e\ j \in \text{Zset}; \forall j \leq (\text{Suc } n). f\ j \in (\text{carrier } K - \{\mathbf{0}\}) \rrbracket \implies$
 $\text{mprod-exp } K\ e\ f\ (\text{Suc } n) = (\text{mprod-exp } K\ e\ f\ n) \cdot_r ((f\ (\text{Suc } n))_K^{(e\ (\text{Suc } n))})$
 ⟨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: $\text{distinct-pds } K n P \implies$
 $(\forall j \leq m. e j \in \text{Zset}) \wedge (\forall j \leq m. 0 \leq (e j)) \wedge$
 $(\forall j \leq m. f j \in \text{carrier } (O_{K P n}) - \{\mathbf{0}_{(O_{K P n})}\}) \longrightarrow$
 $\text{mprod-exp } K e f m = \text{mprod-expR } (O_{K P n}) (\text{nat } o e) f m$
 <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: $\text{valuation } K v \implies$
 $(\forall j \leq n. e j \in \text{Zset}) \wedge (\forall j \leq n. f j \in (\text{carrier } K - \{\mathbf{0}\})) \longrightarrow$
 $v (\text{mprod-exp } K e f n) = \text{ASum } (\lambda j. (e j) *_a (v (f j))) n$
 <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: $\llbracket \text{distinct-pds } K (\text{Suc } n) P;$
 $\text{ideal } (O_{K P (\text{Suc } n)}) I; I \neq \{\mathbf{0}_{(O_{K P (\text{Suc } n)})}\};$
 $I \neq \text{carrier } (O_{K P (\text{Suc } n)}); j \leq (\text{Suc } n) \rrbracket \implies$
 $((\nu_K (P j)) (\text{mprod-exp } K (mL K P I) (Kb_K (\text{Suc } n) P) (\text{Suc } n))) =$
 $((\nu_K (P j)) (\text{Zl-mI } K P I j))$
 <proof>

lemma (in Corps) mgenerator0-2: $\llbracket 0 < n; \text{distinct-pds } K n P; \text{ideal } (O_{K P n}) I;$
 $I \neq \{\mathbf{0}_{(O_{K P n})}\}; I \neq \text{carrier } (O_{K P n}); j \leq n \rrbracket \implies$
 $((\nu_K (P j)) (\text{mprod-exp } K (mL K P I) (Kb_K n P) n)) = ((\nu_K (P j)) (\text{Zl-mI } K P$

$I j)$
 $\langle \text{proof} \rangle$

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

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

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

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

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

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

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

definition
m-zmax-pdsI :: $[-, \text{nat}, \text{nat} \Rightarrow ('b \Rightarrow \text{ant}) \text{ set}, 'b \text{ set}] \Rightarrow \text{int}$ **where**
m-zmax-pdsI $K \ n \ P \ I = (m\text{-zmax } n \ (m\text{-zmax-pdsI-hom } K \ P \ I)) + 1$

lemma (in Corps) *value-Zl-mI-pos*: $\llbracket 0 < n; \ \text{distinct-pds } K \ n \ P; \ \text{ideal } (O_{K \ P \ n}) \ I; \ I \neq \{\mathbf{0}_{(O_{K \ P \ n})}\}; \ I \neq \text{carrier } (O_{K \ P \ n}); \ j \leq n; \ l \leq n \rrbracket \implies$
 $0 \leq ((\nu_K \ (P \ j)) \ (Zl-mI \ K \ P \ I \ l))$
 $\langle \text{proof} \rangle$

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

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

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

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

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

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

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

We write the element $e\Sigma K (\lambda k. (Zl\text{-mI } K P I k) \cdot_K ((\text{mprod-exp } K \text{ (K-gamma } k) \text{ (Kb}_{K n P} \text{) } n)_K^{(m\text{-zmax-pdsI } K n P I)})) n$ 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 ) [82,82,82,83]82) **where**
 $mIg_{K n P I} = \Sigma_e K (\lambda k. (Zl\text{-mI } K P I k) \cdot_r K ((\text{mprod-exp } K \text{ (K-gamma } k) \text{ (Kb}_{K n P} \text{) } n)_K^{(m\text{-zmax-pdsI } K n P I)})) n$

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

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

lemma *not-in-singleton-noneq*: $x \notin \{a\} \implies x \neq a$
 $\langle \text{proof} \rangle$

lemma *noneq-not-in-singleton*: $x \neq a \implies x \notin \{a\}$
 $\langle \text{proof} \rangle$

lemma *inf-neq-1[simp]*: $\infty \neq 1$
 $\langle \text{proof} \rangle$

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

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

lemma *a-p1-gt[simp]*: $\llbracket a \neq \infty; a \neq -\infty \rrbracket \implies a < a + 1$
 $\langle \text{proof} \rangle$

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

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

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

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

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

lemma (**in** *Corps*) *limit-unique*: $\llbracket b \in \text{carrier } K; \forall j. f j \in \text{carrier } K;$

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

definition

v-complete :: $['b \Rightarrow \text{ant}, -] \Rightarrow \text{bool}$
 $((\exists \text{Complete} \text{ - - -}) [90,91]90) \text{ where}$
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 :: $[-, ('b, 'm1) \text{ Ring-scheme}] \Rightarrow \text{bool} \text{ where}$
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 :: $['b \Rightarrow \text{ant}, 'b \Rightarrow \text{ant}, -, ('b, 'm) \text{ Ring-scheme}] \Rightarrow \text{bool}$
 $((\exists \text{Completion} \text{ - - -}) [90,90,90,91]90) \text{ where}$
Completion $_{v v'} K K' \longleftrightarrow \text{subfield } K K' \wedge$

$$\text{Complete}_{v'} K' \wedge (\forall x \in \text{carrier } K. v x = v' x) \wedge \\ (\forall x \in \text{carrier } K'. (\exists f. \text{Cauchy}_K v f \wedge \lim_{K' v'} f x))$$

lemma (in Corps) *subfield-zero*: $\llbracket \text{Corps } K'; \text{subfield } K K' \rrbracket \implies \mathbf{0}_K = \mathbf{0}_{K'}$
 ⟨proof⟩

lemma (in Corps) *subfield-pOp*: $\llbracket \text{Corps } K'; \text{subfield } K K'; x \in \text{carrier } K; \\ y \in \text{carrier } K' \rrbracket \implies x \pm y = x \pm_{K'} y$
 ⟨proof⟩

lemma (in Corps) *subfield-mOp*: $\llbracket \text{Corps } K'; \text{subfield } K K'; x \in \text{carrier } K \rrbracket \implies \\ -_a x = -_a_{K'} x$
 ⟨proof⟩

lemma (in Corps) *completion-val-eq*: $\llbracket \text{Corps } K'; \text{valuation } K v; \text{valuation } K' v'; \\ x \in \text{carrier } K; \text{Completion}_{v v'} K K' \rrbracket \implies v x = v' x$
 ⟨proof⟩

lemma (in Corps) *completion-subset*: $\llbracket \text{Corps } K'; \text{valuation } K v; \text{valuation } K' v'; \\ \text{Completion}_{v v'} K K' \rrbracket \implies \text{carrier } K \subseteq \text{carrier } K'$
 ⟨proof⟩

lemma (in Corps) *completion-subfield*: $\llbracket \text{Corps } K'; \text{valuation } K v; \\ \text{valuation } K' v'; \text{Completion}_{v v'} K K' \rrbracket \implies \text{subfield } K K'$
 ⟨proof⟩

lemma (in Corps) *subfield-sub*: $\text{subfield } K K' \implies \text{carrier } K \subseteq \text{carrier } K'$
 ⟨proof⟩

lemma (in Corps) *completion-Vring-sub*: $\llbracket \text{Corps } K'; \text{valuation } K v; \\ \text{valuation } K' v'; \text{Completion}_{v v'} K K' \rrbracket \implies \\ \text{carrier } (\text{Vr } K v) \subseteq \text{carrier } (\text{Vr } K' v')$
 ⟨proof⟩

lemma (in Corps) *completion-idmap-rHom*: $\llbracket \text{Corps } K'; \text{valuation } K v; \\ \text{valuation } K' v'; \text{Completion}_{v v'} K K' \rrbracket \implies \\ I_{(\text{Vr } K v)} \in \text{rHom } (\text{Vr } K v) (\text{Vr } K' v')$
 ⟨proof⟩

lemma (in Corps) *completion-vpr-sub*: $\llbracket \text{Corps } K'; \text{valuation } K v; \text{valuation } K' v'; \\ \text{Completion}_{v v'} K K' \rrbracket \implies \text{vp } K v \subseteq \text{vp } K' v'$
 ⟨proof⟩

lemma (in Corps) *val-v-completion*: $\llbracket \text{Corps } K'; \text{valuation } K v; \text{valuation } K' v'; \\ x \in \text{carrier } K'; x \neq \mathbf{0}_{K'}; \text{Completion}_{v v'} K K' \rrbracket \implies \\ \exists f. (\text{Cauchy}_K v f) \wedge (\exists N. (\forall m. N < m \longrightarrow v (f m) = v' x))$
 ⟨proof⟩

lemma (in Corps) *v-completion-v-limit*: $\llbracket \text{Corps } K'; \text{valuation } K v;$

$x \in \text{carrier } K; \text{ subfield } K K'; \text{ Complete}_{v'} K'; \forall j. f j \in \text{carrier } K;$
 $\text{valuation } K' v'; \forall x \in \text{carrier } K. v x = v' x; \lim_{K' v'} f x \implies \lim_{K v} f x$
 ⟨proof⟩

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

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

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

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

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

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

⟨proof⟩

lemma (in Corps) res-v-completion-surj:⟦Corps K'; valuation K v;
 valuation K' v'; Completion_{v v'} K K'⟧ \implies
 $\text{surjec}_{(Vr K v), (\text{qrng } (Vr K' v') (vp K' v'))}$
 $(\text{compos } (Vr K v) (\text{pj } (Vr K' v') (vp K' v')) (I_{(Vr K v)}))$

⟨proof⟩

lemma (in Corps) res-v-completion-ker:⟦Corps K'; valuation K v;
 valuation K' v'; Completion_{v v'} K K'⟧ \implies
 $\text{ker}_{(Vr K v), (\text{qrng } (Vr K' v') (vp K' v'))}$
 $(\text{compos } (Vr K v) (\text{pj } (Vr K' v') (vp K' v')) (I_{(Vr K v)})) = vp K v$

⟨proof⟩

lemma (in Corps) completion-res-qrng-isom:⟦Corps K'; valuation K v;
 valuation K' v'; Completion_{v v'} K K'⟧ \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

$Kxa :: [-, 'b \Rightarrow ant, 'b] \Rightarrow 'b \text{ set where}$

$Kxa K v x = \{y. \exists k \in carrier (Vr K v). y = x \cdot_r K k\}$

primrec

$partial\text{-sum} :: [('b, 'm) \text{ Ring-scheme}, 'b, 'b \Rightarrow ant, 'b]$
 $\Rightarrow nat \Rightarrow 'b$

$((5psum \dots) [96,96,96,96,97]96)$

where

$psum\text{-}0: psum K x v t 0 = (csrp\text{-}fn (Vr K v) (vp K v)$
 $(pj (Vr K v) (vp K v) (x \cdot_r K t_K^{- (tna (v x))}))) \cdot_r K (t_K^{(tna (v x))})$

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

definition

$expand\text{-}coeff :: [-, 'b \Rightarrow ant, 'b, 'b]$
 $\Rightarrow nat \Rightarrow 'b$

$((5ecf \dots) [96,96,96,96,97]96) \text{ where}$

$ecf_{K v t x} n = (if n = 0 then csrp\text{-}fn (Vr K v) (vp K v)$

$(pj (Vr K v) (vp K v) (x \cdot_r K t_K^{- (tna (v x))}))$

$else csrp\text{-}fn (Vr K v) (vp K v) (pj (Vr K v)$

$(vp K v) ((x \pm_K -_a K (psum K x v t (n - 1))) \cdot_r K (t_K^{- (tna (v x) + int n))}))))$

definition

$expand\text{-}term :: [-, 'b \Rightarrow ant, 'b, 'b]$
 $\Rightarrow nat \Rightarrow 'b$

$((5etm \dots) [96,96,96,96,97]96) \text{ where}$

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

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

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

$\langle proof \rangle$

lemma (in Corps) Kxa-pow-vpr: $\llbracket valuation K v; t \in carrier K; v t = 1;$

$(0 :: int) \leq j \rrbracket \implies Kxa K v (t_K^j) = (vp K v)^{(Vr K v) (ant j)}$

$\langle proof \rangle$

lemma (in Corps) field-distribTr: $\llbracket a \in carrier K; b \in carrier K;$

$x \in carrier K; x \neq \mathbf{0} \rrbracket \implies a \pm (-_a (b \cdot_r x)) = (a \cdot_r (x^{-K}) \pm (-_a b)) \cdot_r x$

<proof>

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

lemma (in *Corps*) *vp-mem-times-t: [valuation K v; t ∈ carrier K; t ≠ 0;*
v t = 1; x ∈ vp K v] ⇒ ∃ a ∈ carrier (Vr K v). x = a ·_r t
<proof>

lemma (in *Corps*) *psum-diff-mem-Kxa: [valuation K v; t ∈ carrier K;*
v t = 1; x ∈ carrier K; x ≠ 0] ⇒
(psum K x v t n) ∈ carrier K ∧
(x ± (-_a (psum K x v t n))) ∈ Kxa K v (t_K^{((tna (v x)) + (1 + int n))})
<proof>

lemma *Suc-diff-int: 0 < n ⇒ int (n - Suc 0) = int n - 1*
<proof>

lemma (in *Corps*) *ecf-mem: [valuation K v; t ∈ carrier K; v t = 1;*
x ∈ carrier K; x ≠ 0] ⇒ ecf_{K v t x} n ∈ carrier K
<proof>

lemma (in *Corps*) *etm-mem: [valuation K v; t ∈ carrier K; v t = 1;*
x ∈ carrier K; x ≠ 0] ⇒ etm_{K v t x} n ∈ carrier K
<proof>

lemma (in *Corps*) *psum-sum-etm: [valuation K v; t ∈ carrier K; v t = 1;*
x ∈ carrier K; x ≠ 0] ⇒
psum_{K x v t} n = nsum K (λj. (ecf_{K v t x} j)_r (t_K^{(tna (v x) + (int j))})) n
<proof>

lemma *zabs-pos: 0 ≤ (abs (z::int))*
<proof>

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

lemma *zadd-right-mono: (i::int) ≤ j ⇒ i + k ≤ j + k*
<proof>

theorem (in *Corps*) *expansion-thm: [valuation K v; t ∈ carrier K;*
v t = 1; x ∈ carrier K; x ≠ 0] ⇒ lim_{K v} (partial-sum K x v t) x
<proof>

2.9.1 Hensel's theorem

definition

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

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

definition

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

definition

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

definition

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

lemma $an\text{-}neg\text{-}minf[simp]: \forall n. -\infty \neq an n$
 $\langle proof \rangle$

lemma $an\text{-}neg\text{-}minf1[simp]: \forall n. an n \neq -\infty$
 $\langle proof \rangle$

lemma (in Corps) $PseqL\text{-}mem: \llbracket valuation K v; PolynRg R (Vr K v) X;$
 $F n \in carrier R; \forall n. deg R (Vr K v) X (F n) \leq an (Suc d) \rrbracket \implies$
 $(PseqL_R X K v d F) n \in carrier R$
 $\langle proof \rangle$

lemma (in Corps) $Pseqh\text{-}mem: \llbracket valuation K v; PolynRg R (Vr K v) X;$
 $F n \in carrier R; \forall n. deg R (Vr K v) X (F n) \leq an (Suc d) \rrbracket \implies$
 $(Pseqh_R X K v d F) n \in carrier R$
 $\langle proof \rangle$

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

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

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

lemma (in Corps) $v\text{-}ldeg\text{-}p\text{-}pOp$: $[[valuation K v; PolynRg R (Vr K v) X;$
 $p \in carrier R; q \in carrier R; deg R (Vr K v) X p \leq an (Suc d);$
 $deg R (Vr K v) X q \leq an (Suc d)]] \implies$
 $(ldeg\text{-}p R (Vr K v) X d p) \pm_R (ldeg\text{-}p R (Vr K v) X d q) =$
 $ldeg\text{-}p R (Vr K v) X d (p \pm_R q)$
 ⟨proof⟩

lemma (in Corps) $v\text{-}hdeg\text{-}p\text{-}pOp$: $[[valuation K v; PolynRg R (Vr K v) X;$
 $p \in carrier R; q \in carrier R; deg R (Vr K v) X p \leq an (Suc d);$
 $deg R (Vr K v) X q \leq an (Suc d)]] \implies (hdeg\text{-}p R (Vr K v) X (Suc d) p) \pm_R$
 $(hdeg\text{-}p R (Vr K v) X (Suc d) q) = hdeg\text{-}p R (Vr K v) X (Suc d) (p \pm_R q)$
 ⟨proof⟩

lemma (in Corps) $v\text{-}ldeg\text{-}p\text{-}mOp$: $[[valuation K v; PolynRg R (Vr K v) X;$
 $p \in carrier R; deg R (Vr K v) X p \leq an (Suc d)]] \implies$
 $-_aR (ldeg\text{-}p R (Vr K v) X d p) = ldeg\text{-}p R (Vr K v) X d (-_aR p)$
 ⟨proof⟩

lemma (in Corps) $v\text{-}hdeg\text{-}p\text{-}mOp$: $[[valuation K v; PolynRg R (Vr K v) X;$
 $p \in carrier R; deg R (Vr K v) X p \leq an (Suc d)]] \implies$
 $-_aR (hdeg\text{-}p R (Vr K v) X (Suc d) p) = hdeg\text{-}p R (Vr K v) X (Suc d) (-_aR p)$
 ⟨proof⟩

lemma (in Corps) $PCauchy\text{-}lPCauchy$: $[[valuation K v; PolynRg R (Vr K v) X;$
 $\forall n. F n \in carrier R; \forall n. deg R (Vr K v) X (F n) \leq an (Suc d);$
 $P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v)} (an N)) (F n \pm_R -_aR (F m))]]$
 $\implies P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v)} (an N))$
 $((Pseql_R X K v d F) n) \pm_R -_aR ((Pseql_R X K v d F) m))$
 ⟨proof⟩

lemma (in Corps) $PCauchy\text{-}hPCauchy$: $[[valuation K v; PolynRg R (Vr K v) X;$
 $\forall n. F n \in carrier R; \forall n. deg R (Vr K v) X (F n) \leq an (Suc d);$
 $P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v)} (an N)) (F n \pm_R -_aR (F m))]]$
 $\implies P\text{-mod } R (Vr K v) X (vp K v^{(Vr K v)} (an N))$
 $((Pseqh_R X K v d F) n) \pm_R -_aR ((Pseqh_R X K v d F) m))$
 ⟨proof⟩

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

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

lemma (in Corps) monomial-P-limit: \llbracket valuation $K v$; Complete $_v K$;
 PolynRg $R (Vr K v) X$; $\forall n. f n \in \text{carrier } (Vr K v)$;
 $\forall n. F n = (f n) \cdot_{rR} (X^{\sim R} d)$; $\forall N. \exists M. \forall n m. M < n \wedge M < m \implies$
 $P\text{-mod } R (Vr K v) X (vp K v (Vr K v) (an N)) (F n \pm_R \text{--}_a R (F m))$ $\rrbracket \implies$
 $\exists b \in \text{carrier } (Vr K v). \text{Plimit } R X K v F (b \cdot_{rR} (X^{\sim R} d))$
 <proof>

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

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

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

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

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

lemma (in Corps) *Plimit-hdeg*: \llbracket valuation $K v$; PolynRg $R (Vr K v) X$;
 $\forall n. F n \in \text{carrier } R$; $\forall n. \text{deg } R (Vr K v) X (F n) \leq an (Suc d)$;
 $p \in \text{carrier } R$; $Plimit_{R X K v} F p \rrbracket \implies$
 $Plimit_{R X K v} (Pseqh_{R X K v d} F) (hdeg-p R (Vr K v) X (Suc d) p)$
 <proof>

lemma (in Corps) *P-limit-uniqueTr*: \llbracket valuation $K v$; PolynRg $R (Vr K v) X \rrbracket \implies$
 $\forall F. ((\forall n. F n \in \text{carrier } R) \wedge (\forall n. \text{deg } R (Vr K v) X (F n) \leq (an d)) \longrightarrow$
 $(\forall p1 p2. p1 \in \text{carrier } R \wedge p2 \in \text{carrier } R \wedge Plimit_{R X K v} F p1 \wedge$
 $Plimit_{R X K v} F p2 \longrightarrow p1 = p2))$
 <proof>

lemma (in Corps) *P-limit-unique*: \llbracket valuation $K v$; Complete $_v K$;
 PolynRg $R (Vr K v) X$; $\forall n. F n \in \text{carrier } R$;
 $\forall n. \text{deg } R (Vr K v) X (F n) \leq (an d)$; $p1 \in \text{carrier } R$; $p2 \in \text{carrier } R$;
 $Plimit_{R X K v} F p1$; $Plimit_{R X K v} F p2 \rrbracket \implies p1 = p2$
 <proof>

lemma (in Corps) *P-limitTr*: \llbracket valuation $K v$; Complete $_v K$; PolynRg $R (Vr K v) X \rrbracket$
 $\implies \forall F. ((\forall n. F n \in \text{carrier } R) \wedge (\forall n. \text{deg } R (Vr K v) X (F n) \leq (an d)) \wedge$
 $(\forall N. \exists M. \forall n m. M < n \wedge M < m \longrightarrow$
 $P\text{-mod } R (Vr K v) X (vp K v (Vr K v) (an N)) (F n \pm_R -_a R (F m))) \longrightarrow$
 $(\exists p \in \text{carrier } R. Plimit_{R X K v} F p))$
 <proof>

lemma (in Corps) *PCauchy-Plimit*: \llbracket valuation $K v$; Complete $_v K$;
 PolynRg $R (Vr K v) X$; $PCauchy_{R X K v} F \rrbracket \implies$
 $\exists p \in \text{carrier } R. Plimit_{R X K v} F p$
 <proof>

lemma (in Corps) *P-limit-mult*: \llbracket valuation $K v$; PolynRg $R (Vr K v) X$;
 $\forall n. F n \in \text{carrier } R$; $\forall n. G n \in \text{carrier } R$; $p1 \in \text{carrier } R$; $p2 \in \text{carrier } R$;
 $Plimit_{R X K v} F p1$; $Plimit_{R X K v} G p2 \rrbracket \implies$
 $Plimit_{R X K v} (\lambda n. (F n) \cdot_r R (G n)) (p1 \cdot_r R p2)$
 <proof>

definition

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

definition

Hsnd :: $[-, 'b \Rightarrow \text{ant}, ('b, 'm1) \text{ Ring-scheme}, 'b, 'b, ('b \text{ set}, 'm2) \text{ Ring-scheme}, 'b$
 $\text{set}, 'b, 'b, 'b, \text{nat}] \Rightarrow 'b$
 $((11Hsnd \text{ ----- } -) [67,67,67,67,67,67,67,67,67,67,68]67) \text{ where}$

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

lemma (in Corps) Hensel-starter: \llbracket valuation $K v$; Complete $_v K$;
 PolynRg $R (Vr K v) X$; PolynRg $S ((Vr K v) /_r (vp K v)) Y$;
 $t \in \text{carrier } (Vr K v)$; $vp K v = (Vr K v) \diamond_p t$;
 $f \in \text{carrier } R$; $f \neq \mathbf{0}_R$; $g' \in \text{carrier } S$; $h' \in \text{carrier } S$;
 $0 < \text{deg } S ((Vr K v) /_r (vp K v)) Y g'$;
 $0 < \text{deg } S ((Vr K v) /_r (vp K v)) Y h'$;
 $((erH R (Vr K v) X S ((Vr K v) /_r (vp K v)) Y$
 $(pj (Vr K v) (vp K v))) f) = g' \cdot_r S h'$;
 rel-prime-pols $S ((Vr K v) /_r (vp K v)) Y g' h'$ $\rrbracket \implies$
 $\exists g h. g \neq \mathbf{0}_R \wedge h \neq \mathbf{0}_R \wedge g \in \text{carrier } R \wedge h \in \text{carrier } R \wedge$
 $\text{deg } R (Vr K v) X g \leq \text{deg } S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$
 $(erH R (Vr K v) X S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$
 $(pj (Vr K v) ((Vr K v) \diamond_p t)) g) \wedge (\text{deg } R (Vr K v) X h +$
 $\text{deg } S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y (erH R (Vr K v) X S$
 $((Vr K v) /_r ((Vr K v) \diamond_p t)) Y (pj (Vr K v) ((Vr K v) \diamond_p t)) g)$
 $\leq \text{deg } R (Vr K v) X f) \wedge$
 $(erH R (Vr K v) X S ((Vr K v) /_r (vp K v)) Y$
 $(pj (Vr K v) (vp K v))) g = g' \wedge$
 $(erH R (Vr K v) X S ((Vr K v) /_r (vp K v)) Y$
 $(pj (Vr K v) (vp K v))) h = h' \wedge$
 $0 < \text{deg } S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$
 $(erH R (Vr K v) X S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$
 $(pj (Vr K v) ((Vr K v) \diamond_p t)) g) \wedge$
 $0 < \text{deg } S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$
 $(erH R (Vr K v) X S ((Vr K v) /_r ((Vr K v) \diamond_p t)) Y$
 $(pj (Vr K v) ((Vr K v) \diamond_p t)) h) \wedge$
 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: $\llbracket a \leq (a'::\text{ant}); b \leq b' \rrbracket \implies a + b \leq a' + b'$
 $\langle \text{proof} \rangle$

lemma (in Corps) Hfst-PCauchy: \llbracket valuation $K v$; Complete $_v K$;
 PolynRg $R (Vr K v) X$; PolynRg $S (Vr K v /_r (Vr K v \diamond_p t)) Y$; $g0 \in \text{carrier}$
 R ;
 $h0 \in \text{carrier } R$; $f \in \text{carrier } R$; $f \neq \mathbf{0}_R$; $g0 \neq \mathbf{0}_R$; $h0 \neq \mathbf{0}_R$;
 $t \in \text{carrier } (Vr K v)$; $vp K v = Vr K v \diamond_p t$;
 $\text{deg } R (Vr K v) X g0 \leq \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (erH R (Vr K v) X S$
 $(Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0)$;
 $\text{deg } R (Vr K v) X h0 + \text{deg } S (Vr K v /_r (Vr K v \diamond_p t)) Y (erH R (Vr K v) X$
 S
 $(Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0)$
 $\leq \text{deg } R (Vr K v) X f$;

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

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

\langle proof \rangle

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

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

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

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

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

$\deg R (Vr K v) X h0 + \deg S (Vr K v /_r (Vr K v \diamond_p t)) Y (erH R (Vr K v) X$
 S

$(Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0)$
 $\leq \deg R (Vr K v) X f$;

$0 < \deg S (Vr K v /_r (Vr K v \diamond_p t)) Y (erH R (Vr K v) X S$
 $(Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) g0)$;

$0 < \deg S (Vr K v /_r (Vr K v \diamond_p t)) Y (erH R (Vr K v) X S$
 $(Vr K v /_r (Vr K v \diamond_p t)) Y (pj (Vr K v) (Vr K v \diamond_p t)) h0)$;

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

$(erH R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y$
 $(pj (Vr K v) (Vr K v \diamond_p t)) h0)$;

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

$(pj (Vr K v) (Vr K v \diamond_p t)) f =$

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

$(pj (Vr K v) (Vr K v \diamond_p t)) g0 \cdot_r S$

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

$(pj (Vr K v) (Vr K v \diamond_p t)) h0 \implies$

$PCauchy R X K v Hsnd K v R X t S Y f g0 h0$

\langle proof \rangle

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

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

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

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

$erH R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y$
 $(pj (Vr K v) (Vr K v \diamond_p t)) f =$
 $erH R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y$
 $(pj (Vr K v) (Vr K v \diamond_p t)) g0 \cdot_r S$
 $erH R (Vr K v) X S (Vr K v /_r (Vr K v \diamond_p t)) Y$
 $(pj (Vr K v) (Vr K v \diamond_p t)) h0$;

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

$g \in \text{carrier } R$; $h \in \text{carrier } R$;
 $Plimit R X K v (Hfst K v R X t S Y f g0 h0) g$;
 $Plimit R X K v (Hsnd K v R X t S Y f g0 h0) h$;
 $Plimit R X K v (\lambda n. (Hfst K v R X t S Y f g0 h0 n) \cdot_r R$
 $(Hsnd K v R X t S Y f g0 h0 n)) (g \cdot_r R h)]$
 $\implies Plimit R X K v (\lambda n. (Hfst K v R X t S Y f g0 h0 n) \cdot_r R$
 $(Hsnd K v R X t S Y f g0 h0 n)) f$

<proof>

theorem (in Corps) Hensel: $\llbracket \text{valuation } K v$; $\text{Complete}_v K$;
 $PolynRg R (Vr K v) X$; $PolynRg S ((Vr K v) /_r (vp K v)) Y$;
 $f \in \text{carrier } R$; $f \neq \mathbf{0}_R$; $g' \in \text{carrier } S$; $h' \in \text{carrier } S$;
 $0 < \text{deg } S ((Vr K v) /_r (vp K v)) Y g'$;
 $0 < \text{deg } S ((Vr K v) /_r (vp K v)) Y h'$;
 $((erH R (Vr K v) X S ((Vr K v) /_r (vp K v)) Y$
 $(pj (Vr K v) (vp K v))) f) = g' \cdot_r S h'$;

$$\begin{aligned}
& \text{rel-prime-pols } S \ ((Vr\ K\ v) /_r (vp\ K\ v))\ Y\ g'\ h' \rceil \implies \\
& \exists g\ h. g \in \text{carrier } R \wedge h \in \text{carrier } R \wedge \\
& \quad \text{deg } R\ (Vr\ K\ v)\ X\ g \leq \text{deg } S \ ((Vr\ K\ v) /_r (vp\ K\ v))\ Y\ g' \wedge \\
& \quad \quad f = g \cdot_{\tau R} h
\end{aligned}$$

<proof>

end