Contents

Chapter 1

Real Analysis

(1.5)
$OrderTrichotomy[<, S] := \forall_{x,y\in S}(x < y \veebar x = y \veebar y < x)$
$OrderTransitivity[<, S] := \forall_{x,y,z\in S}\big((x < y \wedge y < z) \implies x < z\big)$
$Order[<, S] := (OrderTrichotomy[<, S]) \wedge (OrderTransitivity[<, S])$

(1.7)
$BoundedAbove[E, S, <] := (Order[<, S]) \wedge (E \subset S) \wedge \Big(\exists_{\beta\in S}\forall_{x\in E}(x \leq \beta)\Big)$
$BoundedBelow[E, S, <] := (Order[<, S]) \wedge (E \subset S) \wedge \Big(\exists_{\beta\in S}\forall_{x\in E}(\beta \leq x)\Big)$
$UpperBound[\beta, E, S, <] := (Order[<, S]) \wedge (E \subset S) \wedge \big(\beta \in S \wedge \forall_{x\in E}(x \leq \beta)\big)$
$LowerBound[\beta, E, S, <] := (Order[<, S]) \wedge (E \subset S) \wedge \big(\beta \in S \wedge \forall_{x\in E}(\beta \leq x)\big)$

(1.8)
$LUB[\alpha, E, S, <] := (UpperBound[\alpha, E, S, <]) \wedge \Big(\forall_\gamma(\gamma < \alpha \implies \neg UpperBound[\gamma, E, S, <])\Big)$
$GLB[\alpha, E, S, <] := (LowerBound[\alpha, E, S, <]) \wedge \Big(\forall_\beta(\alpha < \beta \implies \neg LowerBound[\beta, E, S, <])\Big)$

(1.10)
$LUBProperty[S, <] := \forall_E\Big(\big((\emptyset \neq E \subset S) \wedge (BoundedAbove[E, S, <]) \implies \exists_{\alpha\in S}(LUB[\alpha, E, S, <])\big)\Big)$
$GLBProperty[S, <] := \forall_E\Big(\big((\emptyset \neq E \subset S) \wedge (BoundedBelow[E, S, <]) \implies \exists_{\alpha\in S}(GLB[\alpha, E, S, <])\big)\Big)$

(1.11)
$LUBPropertyImpliesGLBProperty := LUBProperty[S, <] \implies GLBProperty[S, <]$

---

(1) $LUBProperty[S, <] \implies \ldots$ — wts: 2

(1.1) $(\emptyset \neq B \subset S \wedge BoundedBelow[B, S, <]) \implies \ldots$ — wts: 1.2

(1.1.1) $Order[<, S] \wedge \exists_{\delta'\in S}(LowerBound[\delta', B, S, <])$ — from: $BoundedBelow$, 1.1

(1.1.2) $|B| = 1 \implies \ldots$ — wts: 1.1.3

(1.1.2.1) $\exists_{u'}(u' \in B) \;\blacksquare\; u := choice(\{u' : u' \in B\}) \;\blacksquare\; B = \{u\}$ — from: 1.1.2

(1.1.2.2) $GLB[u, B, S, <] \;\blacksquare\; \exists_{\epsilon_0\in S}(GLB[\epsilon_0, B, S, <])$

(1.1.3) $|B| = 1 \implies \exists_{\epsilon_0\in S}(GLB[\epsilon_0, B, S, <])$

(1.1.4) $|B| \neq 1 \implies \ldots$ — wts: 1.1.5

(1.1.4.1) $\forall_E\big((\emptyset \neq E \subset S \wedge BoundedAbove[E, S, <]) \implies \exists_{\alpha\in S}(LUB[\alpha, E, S, <])\big)$ — from: $LUBProperty$, 1

(1.1.4.2) $L := \{s \in S : LowerBound[s, B, S, <]\}$

(1.1.4.3) $|B| > 1 \wedge OrderTrichotomy[<, S] \;\blacksquare\; \exists_{b_1{}'\in B}\exists_{b_0{}'\in B}(b_0{}' < b_1{}')$ — from: $Order$, 1.1.1; wts: 1.1.4.7

(1.1.4.4) $b_1 := choice\Big(\{b_1{}' \in B : \exists_{b_0{}'\in B}(b_0{}' < b_1{}')\}\Big) \;\blacksquare\; \neg LowerBound[b_1, B, S, <]$ — from: 1.1.4.2

(1.1.4.5) $b_1 \notin L \;\blacksquare\; L \subset S$

(1.1.4.6) $\delta := choice(\{\delta' \in S : LowerBound[\delta', B, S, <]\}) \;\blacksquare\; \delta \in L \;\blacksquare\; \emptyset \neq L$ — from: 1.1.1

(1.1.4.7) $\emptyset \neq L \subset S$ — from: 1.1.4.5, 1.1.4.6

(1.1.4.8) $\forall_{y\in L}(LowerBound[y_0, B, S, <]) \;\blacksquare\; \forall_{y\in L}\forall_{x\in B}(y_0 \leq x)$ — from: $LowerBound$, 1.1.4.2; wts: 1.1.4.10

(1.1.4.9) $\forall_{x \in B}\Big(x \in S \wedge \forall_{y \in L}(y_0 \leq x)\Big) \blacksquare \forall_{x \in B}(UpperBound[x, L, S, <])$ from: UpperBound

(1.1.4.10) $\exists_{x \in S}(UpperBound[x, L, S, <]) \blacksquare BoundedAbove[L, S, <]$

(1.1.4.11) $\emptyset \neq L \subset S \wedge BoundedAbove[L, S, <]$ from: 1.1.4.7, 1.1.4.10

(1.1.4.12) $\exists_{\alpha' \in S}(LUB[\alpha', L, S, <]) \blacksquare \alpha := choice\Big(\{\alpha' \in S : (LUB[\alpha', L, S, <])\}\Big)$ from: 1.1.4.1 wts: 1.1.4.21

(1.1.4.13) $\forall_x(x \in B \implies UpperBound[x, L, S, <])$ from: 1.1.4.9 wts: 1.1.4.17

(1.1.4.14) $\forall_x(\neg UpperBound[x, L, S, <] \implies x \notin B)$

(1.1.4.15) $\gamma < \alpha \implies \ldots$ wts: 1.1.4.16

(1.1.4.15.1) $\neg UpperBound[\gamma, L, S, <] \blacksquare \gamma \notin B$ from: LUB, 1.1.4.12, 1.1.4.14

(1.1.4.16) $\gamma < \alpha \implies \gamma \notin B \blacksquare \gamma \in B \implies \gamma \geq \alpha$

(1.1.4.17) $\forall_{\gamma \in B}(\alpha \leq \gamma) \blacksquare LowerBound[\alpha, B, S, <]$ from: LowerBound

(1.1.4.18) $\alpha < \beta \implies \ldots$ wts: 1.1.4.19

(1.1.4.18.1) $\forall_{y \in L}(y_0 \leq \alpha < \beta) \blacksquare \forall_{y \in L}(y_0 \neq \beta)$ from: LUB, 1.1.4.12, 1.1.4.18

(1.1.4.18.2) $\beta \notin L \blacksquare \neg LowerBound[\beta, B, S, <]$ from: 1.1.4.2

(1.1.4.19) $\alpha < \beta \implies \neg LowerBound[\beta, B, S, <] \blacksquare \forall_{\beta \in S}(\alpha < \beta \implies \neg LowerBound[\beta, B, S, <])$

(1.1.4.20) $LowerBound[\alpha, B, S, <] \wedge \forall_{\beta \in S}(\alpha < \beta \implies \neg LowerBound[\beta, B, S, <])$ from: 1.1.4.17, 1.1.4.19

(1.1.4.21) $GLB[\alpha, B, S, <] \blacksquare \exists_{\epsilon_1 \in S}(GLB[\epsilon_1, B, S, <])$

(1.1.5) $|B| \neq 1 \implies \exists_{\epsilon_1 \in S}(GLB[\epsilon_1, B, S, <])$

(1.1.6) $\Big(|B| = 1 \implies \exists_{\epsilon_0 \in S}(GLB[\epsilon_0, B, S, <])\Big) \wedge \Big(|B| \neq 1 \implies \exists_{\epsilon_1 \in S}(GLB[\epsilon_1, B, S, <])\Big)$ from: 1.1.3, 1.1.5

(1.1.7) $(|B| = 1 \vee |B| \neq 1) \implies \exists_{\epsilon \in S}(GLB[\epsilon, B, S, <]) \blacksquare \exists_{\epsilon \in S}(GLB[\epsilon, B, S, <])$

(1.2) $(\emptyset \neq B \subset S \wedge BoundedBelow[B, S, <]) \implies \exists_{\epsilon \in S}(GLB[\epsilon, B, S, <])$

(1.3) $\forall_B\Big((\emptyset \neq B \subset S \wedge BoundedBelow[B, S, <]) \implies \exists_{\epsilon \in S}(GLB[\epsilon, B, S, <])\Big)$

(1.4) $GLBProperty[S, <]$

(2) $LUBProperty[S, <] \implies GLBProperty[S, <]$

(1.12)

$$Field[F, +, *] := \exists_{0,1 \in F}\forall_{x,y,z \in F}\left(\begin{array}{l} x + y \in F \quad \wedge \quad x * y \in F \quad \wedge \\ x + y = y + x \quad \wedge \quad x * y = y * x \quad \wedge \\ (x + y) + z = x + (y_0 + z) \quad \wedge \quad (x * y) * z = x * (y_0 * z) \quad \wedge \\ \mathbb{1} \neq \mathbb{0} \quad \wedge \quad x * (y_0 + z) = (x * y) + (x * z) \quad \wedge \\ \mathbb{0} + x = x \quad \wedge \quad \mathbb{1} * x = x \quad \wedge \\ \exists_{-x \in F}\big(x + (-x) = \mathbb{0}\big) \wedge \Big(x \neq \mathbb{0} \implies \exists_{1/x \in F}\big(x * (1/x) = \mathbb{1}\big)\Big) \end{array}\right)$$

************************ $(Field[F, +, *] \wedge x, y, z \in F) \implies \ldots$ ************************

(1.14)

$AdditiveCancellation := (x + y = x + z) \implies y = z$

(1) $y = \mathbb{0} + y = \big(x + (-x)\big) + y = \big((-x) + x\big) + y = (-x) + (x + y) = \ldots$ from: Field

(2) $(-x) + (x + z) = \big((-x) + x\big) + z = \big(x + (-x)\big) + z = \mathbb{0} + z = z$ from: Field

$AdditiveIdentityUniqueness := (x + y = x) \implies y = \mathbb{0}$

(1) $x + y = x = \mathbb{0} + x = x + \mathbb{0}$ from: Field

(2) $y = 0$ from: AdditiveCancellation

$AdditiveInverseUniqueness := (x + y = \mathbb{0}) \implies y = -x$

(1) $x + y = \mathbb{0} = x + (-x)$ from: Field

(2) $y = -x$ from: AdditiveCancellation

$DoubleNegative := x = -(-x)$

(1) $\mathbb{0} = x + (-x) = (-x) + x \blacksquare \mathbb{0} = (-x) + x$ from: Field

from: $AdditiveInverseUniqueness$

(2) $x = -(-x)$

(1.15)

$MultiplicativeCancellation := (x \neq 0 \wedge x * y = x * z) \implies y = z$ —

$MultiplicativeIdentityUniqueness := (x \neq 0 \wedge x * y = x) \implies y = \mathbb{1}$ —

$MultiplicativeInverseUniqueness := (x \neq 0 \wedge x * y = \mathbb{1}) \implies y = 1/x$ —

$DoubleReciprocal := (x \neq 0) \implies x = 1/(1/x)$ —

(1.16)

$Domination := \mathbb{0} * x = \mathbb{0}$

from: $Field$

(1) $\mathbb{0} * x = (\mathbb{0} + \mathbb{0}) * x = \mathbb{0} * x + \mathbb{0} * x$ ▮ $\mathbb{0} * x = \mathbb{0} * x + \mathbb{0} * x$

from: $AdditiveIdentityUniqueness$

(2) $\mathbb{0} * x = \mathbb{0}$

$NonDomination := (x \neq \mathbb{0} \wedge y \neq \mathbb{0}) \implies x * y \neq \mathbb{0}$

(1) $(x \neq \mathbb{0} \wedge y \neq \mathbb{0}) \implies \ldots$

(1.1) $(x * y = 0) \implies \ldots$

from: $Field$, $Domination$, 1, 1.1

(1.1.1) $\mathbb{1} = \mathbb{1} * \mathbb{1} = \big(x * (1/x)\big) * \big(y * (1/y)\big) = (x * y) * \big((1/x) * (1/y)\big) = \mathbb{0} * \big((1/x) * (1/y)\big) = \mathbb{0}$

from: $Field$

(1.1.2) $\mathbb{1} = \mathbb{0} \wedge \mathbb{1} \neq \mathbb{0}$ ▮ $\perp$

(1.2) $(x * y = 0) \implies \perp$ ▮ $x * y \neq 0$

(2) $(x \neq \mathbb{0} \wedge y \neq \mathbb{0}) \implies x * y \neq 0$

$NegationCommutativity := (-x) * y = -(x * y) = x * (-y)$

from: $Field$, $Domination$
wts: 2

(1) $x * y + (-x) * y = (x + -x) * y = \mathbb{0} * y = \mathbb{0}$ ▮ $x * y + (-x) * y = \mathbb{0}$

from: $AdditiveInverseUniqueness$

(2) $(-x) * y = -(x * y)$

from: $Field$, $Domination$
wts: 4

(3) $x * y + x * (-y) = x * (y_0 + -y) = x * \mathbb{0} = \mathbb{0}$ ▮ $x * y + x * (-y) = \mathbb{0}$

from: $AdditiveInverseUniqueness$

(4) $x * (-y) = -(x * y)$

from: 2, 4

(5) $(-x) * y = -(x * y) = x * (-y)$

$NegativeMultiplication := (-x) * (-y) = x * y$

from: $NegationCommutativity$, $DoubleNegative$

(1) $(-x) * (-y) = -\big(x * (-y)\big) = -\big(-(x * y)\big) = x * y$

(1.17)

$$OrderedField[F, +, *, <] := \begin{pmatrix} Field[F, +, *] \quad \wedge \quad Order[<, F] \quad \wedge \\ \forall_{x,y,z \in F}(y_0 < z \implies x + y < x + z) \wedge \\ \forall_{x,y \in F}\big((x > \mathbb{0} \wedge y > \mathbb{0}) \implies x * y > \mathbb{0}\big) \end{pmatrix}$$

************************ $(OrderedField[F, +, *, <] \wedge x, y, z \in F) \implies \ldots$ ************************

(1.18)

$NegationOnOrder := x > \mathbb{0} \iff -x < \mathbb{0}$

(1) $x > \mathbb{0} \implies \ldots$

from: $OrderedField$

(1.1) $\mathbb{0} = (-x) + x > (-x) + \mathbb{0} = -x$ ▮ $\mathbb{0} > -x$ ▮ $-x < \mathbb{0}$

(2) $x > \mathbb{0} \implies -x < \mathbb{0}$

(3) $-x < \mathbb{0} \implies \ldots$

from: $OrderedField$

(3.1) $\mathbb{0} = x + (-x) < x + \mathbb{0} = x$ ▮ $\mathbb{0} < x$ ▮ $x > \mathbb{0}$

(4) $-x < \mathbb{0} \implies x > \mathbb{0}$

from: 2, 4

(5) $x > \mathbb{0} \implies -x < \mathbb{0} \wedge -x < \mathbb{0} \implies x > \mathbb{0}$ ▮ $x > \mathbb{0} \iff -x < \mathbb{0}$

$PositiveFactorPreservesOrder := (x > \mathbb{0} \wedge y < z) \implies x * y < x * z$

(1) $(x > \mathbb{0} \wedge y < z) \implies \ldots$

from: $OrderedField$

(1.1) $(-y) + z > (-y) + y = \mathbb{0}$ ▮ $z + (-y) = \mathbb{0}$

from: $OrderedField$

(1.2) $x * \big(z + (-y)\big) > \mathbb{0}$ ▮ $x * z + x * (-y) > \mathbb{0}$

(1.3) $x * z = \mathbb{0} + x * z = \big(x * y + -(x * y)\big) + x * z = \big(x * y + x * (-y)\big) + x * z = \ldots$ from: *Field*, *NegationCommutativity*

(1.4) $x * y + \big(x * z + x * (-y)\big) > x * y + \mathbb{0} = x * y$ from: *Field*, 1.2

(1.5) $x * z > x * y$ from: 1.3, 1.4

(2) $(x > \mathbb{0} \wedge y < z) \implies x * z > x * y$

$NegativeFactorFlipsOrder := (x < \mathbb{0} \wedge y < z) \implies x * y > x * z$

(1) $(x < \mathbb{0} \wedge y < z) \implies \ldots$

(1.1) $-x > \mathbb{0}$ from: *NegationOnOrder*

(1.2) $(-x) * y < (-x) * z \;\blacksquare\; \mathbb{0} = x * y + (-x) * y < x * y + (-x) * z \;\blacksquare\; \mathbb{0} < x * y + (-x) * z$ from: *PositiveFactorPreservesOrder*

(1.3) $\mathbb{0} < (-x) * (-y + z) \;\blacksquare\; \mathbb{0} > x * (-y + z) \;\blacksquare\; \mathbb{0} > -(x * y) + x * z$ from: *NegationOnOrder*

(1.4) $x * y > x * z$

(2) $(x < \mathbb{0} \wedge y < z) \implies x * y > x * z$

$SquareIsPositive := (x \neq \mathbb{0}) \implies x * x > \mathbb{0}$

(1) $(x > \mathbb{0}) \implies x * x > 0$ from: *OrderedField*

(2) $(x < \mathbb{0}) \implies \ldots$

(2.1) $-x > \mathbb{0} \;\blacksquare\; x * x = (-x) * (-x) > \mathbb{0} \;\blacksquare\; x * x > \mathbb{0}$ from: *NegationOnOrder*, *OrderedField*, *NegativeMultiplication*

(3) $(x < \mathbb{0}) \implies x * x > \mathbb{0}$

(4) $x \neq \mathbb{0} \implies (x > \mathbb{0} \vee x < \mathbb{0}) \implies x * x > \mathbb{0} \;\blacksquare\; x \neq \mathbb{0} \implies x * x > \mathbb{0}$ from: *OrderTrichotomy*, 1, 3

$OneIsPositive := \mathbb{1} > \mathbb{0}$

(1) $\mathbb{1} \neq \mathbb{0} \;\blacksquare\; \mathbb{1} = \mathbb{1} * \mathbb{1} > \mathbb{0}$ from: *Field*, *SquareIsPositive*

$ReciprocationOnOrder := (0 < x < y) \implies 0 < 1/y < 1/x$

(1) $(0 < x < y) \implies \ldots$

(1.1) $x * (1/x) = \mathbb{1} > \mathbb{0} \;\blacksquare\; x * (1/x) > 0$ from: *Field*, *OneIsPositive*

(1.2) $1/x < \mathbb{0} \implies x * (1/x) < 0 \wedge x * (1/x) > 0 \implies \perp \;\blacksquare\; 1/x > \mathbb{0}$ from: *NegativeFactorFlipsOrder*, 1

(1.3) $y * (1/y) = \mathbb{1} > \mathbb{0} \;\blacksquare\; y * (1/y) > 0$ from: *Field*, *OneIsPositive*

(1.4) $1/y < \mathbb{0} \implies y * (1/y) < 0 \wedge y * (1/y) > 0 \implies \perp \;\blacksquare\; 1/y > \mathbb{0}$ from: *NegativeFactorFlipsOrder*, 1

(1.5) $(1/x) * (1/y) > \mathbb{0}$ from: *OrderedField*

(1.6) $\mathbb{0} < 1/y = \big((1/x) * (1/y)\big) * x < \big((1/x) * (1/y)\big) * y = 1/x$ from: *OrderedField*, 1, 1.4, 1.5

(1.19)

$OrderedFieldQ := OrderedField[\mathbb{Q}, +, *, <]$ —

$Subfield[K, F, +, *] := Field[F, +, *] \wedge K \subset F \wedge Field[K, +, *]$

$OrderedSubfield[K, F, +, *, <] := OrderedField[F, +, *, <] \wedge K \subset F \wedge OrderedField[K, +, *, <]$

$CutI[\alpha] := \emptyset \neq \alpha \subset \mathbb{Q}$

$CutII[\alpha] := \forall_{p \in \alpha} \forall_{q \in \mathbb{Q}} (q < p \implies q \in \alpha)$

$CutIII[\alpha] := \forall_{p \in \alpha} \exists_{r \in \alpha} (p < r)$

$\mathbb{R} := \{\alpha \in \mathbb{Q} : CutI[\alpha] \wedge CutII[\alpha] \wedge CutIII[\alpha]\}$

$CutCorollaryI := (\alpha \in \mathbb{R} \wedge p \in \alpha \wedge q \in \mathbb{Q} \wedge q \notin \alpha) \implies p < q$

(1) $(\alpha \in \mathbb{R} \wedge p \in \alpha \wedge q \in \mathbb{Q} \wedge q \notin \alpha) \implies \ldots$

(1.1) $\forall_{p' \in \alpha} \forall_{q' \in \mathbb{Q}} (q' < p' \implies q' \in \alpha)$ from: *CutII*, 1

(1.2) $q < p \implies q \in \alpha \;\blacksquare\; q \notin \alpha \implies q \geq p$ from: 1

(1.3) $(q \notin \alpha) \implies \ldots$

(1.3.1) $q \geq p$ from: 1.2

(1.3.2) $(q = p) \implies (p \in \alpha \wedge p \notin \alpha) \implies \perp \;\blacksquare\; q \neq p$ from: 1, 1.3

(1.3.3) $q \geq p \wedge q \neq p \;\blacksquare\; p < q$

(1.4) $q \notin \alpha \implies p < q \;\blacksquare\; p < q$ from: 1

(2) $(\alpha \in \mathbb{R} \wedge p \in \alpha \wedge q \in \mathbb{Q} \wedge q \notin \alpha) \implies p < q$

$\mathit{CutCorollaryII} := (\alpha \in \mathbb{R} \wedge r, s \in \mathbb{Q} \wedge r < s \wedge r \notin \alpha) \implies s \notin \alpha$

(1) $(\alpha \in \mathbb{R} \wedge r, s \in \mathbb{Q} \wedge r < s \wedge r \notin \alpha) \implies \ldots$

(1.1) $\forall_{s' \in \alpha} \forall_{r' \in \mathbb{Q}} (r' < s' \implies r' \in \alpha)$ from: *CutII*, 1

(1.2) $s \in \alpha \implies \big(r \in \mathbb{Q} \implies (r < s \implies r \in \alpha)\big) \;\blacksquare\; s \in \alpha \implies r \in \alpha$ from: 1, 1.1

(1.3) $r \notin \alpha \implies s \notin \alpha \;\blacksquare\; s \notin \alpha$ from: 1, 1.2

(2) $(\alpha \in \mathbb{R} \wedge r, s \in \mathbb{Q} \wedge r < s \wedge r \notin \alpha) \implies s \notin \alpha$

$<_{\mathbb{R}}[\alpha, \beta] := \alpha, \beta \in \mathbb{R} \wedge \alpha \subset \beta$

$\mathit{OrderTrichotomyOfR} := \mathit{OrderTrichotomy}[\mathbb{R}, <_{\mathbb{R}}]$

(1) $(\alpha, \beta \in \mathbb{R}) \implies \ldots$

(1.1) $\neg(\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta) \implies \ldots$

(1.1.1) $\alpha \not\subset \beta \wedge \alpha \neq \beta$ from: $<_{\mathbb{R}}$, 1.1

(1.1.2) $\exists_{p'}(p' \in \alpha \wedge p' \notin \beta) \;\blacksquare\; p := \mathit{choice}(\{p' : p' \in \alpha \wedge p' \notin \beta\})$

(1.1.3) $q \in \beta \implies \ldots$

(1.1.3.1) $p, q \in \mathbb{Q}$

(1.1.3.2) $q < p$ from: *CutCorollaryI*

(1.1.3.3) $q \in \alpha$ from: *CutII*

(1.1.4) $q \in \beta \implies q \in \alpha$

(1.1.5) $\forall_{q \in \beta}(q \in \alpha) \;\blacksquare\; \beta \subseteq \alpha$

(1.1.6) $\beta \subset \alpha \;\blacksquare\; \beta <_{\mathbb{R}} \alpha$

(1.2) $\neg(\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta) \implies \beta <_{\mathbb{R}} \alpha$

(1.3) $\neg(\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta) \vee (\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta) \;\blacksquare\; (\beta <_{\mathbb{R}} \alpha) \vee (\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta)$

(1.4) $\alpha = \beta \implies \neg(\alpha <_{\mathbb{R}} \beta \vee \beta <_{\mathbb{R}} \alpha)$

(1.5) $\alpha <_{\mathbb{R}} \beta \implies \neg(\alpha = \beta \vee \beta <_{\mathbb{R}} \alpha)$

(1.6) $\beta <_{\mathbb{R}} \alpha \implies \neg(\alpha = \beta \vee \alpha <_{\mathbb{R}} \beta)$

(1.7) $\alpha <_{\mathbb{R}} \beta \veebar \alpha = \beta \veebar \alpha <_{\mathbb{R}} \beta$

(2) $(\alpha, \beta \in \mathbb{R}) \implies (\alpha <_{\mathbb{R}} \beta \veebar \alpha = \beta \veebar \alpha <_{\mathbb{R}} \beta)$

(3) $\forall_{\alpha, \beta \in \mathbb{R}}(\alpha <_{\mathbb{R}} \beta \veebar \alpha = \beta \veebar \alpha <_{\mathbb{R}} \beta)$

(4) $\mathit{OrderTrichotomy}[\mathbb{R}, <_{\mathbb{R}}]$

$\mathit{OrderTransitivityOfR} := \mathit{OrderTransitivity}[\mathbb{R}, <_{\mathbb{R}}]$

(1) $(\alpha, \beta, \gamma \in \mathbb{R}) \implies \ldots$

(1.1) $(\alpha <_{\mathbb{R}} \beta \wedge \beta <_{\mathbb{R}} \gamma) \implies \ldots$

(1.1.1) $\alpha \subset \beta \wedge \beta \subset \gamma$

(1.1.2) $\forall_{a \in \alpha}(a \in \beta) \wedge \forall_{b \in \beta}(b \in \gamma)$

(1.1.3) $\forall_{a \in \alpha}(\alpha \in \gamma) \;\blacksquare\; \alpha \subset \gamma \;\blacksquare\; \alpha <_{\mathbb{R}} \gamma$

(1.2) $(\alpha <_{\mathbb{R}} \beta \wedge \beta <_{\mathbb{R}} \gamma) \implies \alpha <_{\mathbb{R}} \gamma$

(2) $(\alpha, \beta, \gamma \in \mathbb{R}) \implies \big((\alpha <_{\mathbb{R}} \beta \wedge \beta <_{\mathbb{R}} \gamma) \implies \alpha <_{\mathbb{R}} \gamma\big)$

(3) $\forall_{\alpha, \beta, \gamma \in \mathbb{R}}\big((\alpha <_{\mathbb{R}} \beta \wedge \beta <_{\mathbb{R}} \gamma) \implies \alpha <_{\mathbb{R}} \gamma\big)$

(4) $\mathit{OrderTransitivity}[\mathbb{R}, <_{\mathbb{R}}]$

$\mathit{OrderOfR} := \mathit{Order}[<_{\mathbb{R}}, \mathbb{R}]$ from: *OrderTrichotomyR*, *OrderTransitivityR*

wts:

$\mathit{LUBPropertyOfR} := \mathit{LUBProperty}[\mathbb{R}, <_{\mathbb{R}}]$

(1) $(\emptyset \neq A \subset \mathbb{R} \wedge \mathit{BoundedAbove}[A, \mathbb{R}, <_{\mathbb{R}}]) \implies \ldots$

(1.1) $\gamma := \{p \in \mathbb{Q} : \exists_{\alpha \in A}(p \in \alpha)\}$

(1.2) $A \neq \emptyset \;\blacksquare\; \exists_{\alpha}(\alpha \in A) \;\blacksquare\; \alpha_0 := choice(\{\alpha : \alpha \in A\})$

(1.3) $\alpha_0 \neq \emptyset \;\blacksquare\; \exists_a(a \in \alpha_0) \;\blacksquare\; a_0 := choice(\{a : a \in \alpha_0\}) \;\blacksquare\; a_0 \in \gamma \;\blacksquare\; \gamma \neq \emptyset$

(1.4) $\mathit{BoundedAbove}[A, \mathbb{R}, <_{\mathbb{R}}] \;\blacksquare\; \exists_{\beta}(\mathit{UpperBound}[\beta, A, \mathbb{R}, <_{\mathbb{R}}])$

(1.5) $\beta_0 := choice(\{\beta : \mathit{UpperBound}[\beta, A, \mathbb{R}, <_{\mathbb{R}}]\})$

(1.6) $\mathit{UpperBound}[\beta_0, A, \mathbb{R}, <_{\mathbb{R}}] \;\blacksquare\; \forall_{\alpha\in A}(\alpha \leq_{\mathbb{R}} \beta_0) \;\blacksquare\; \forall_{\alpha\in A}(\alpha \subseteq \beta_0) \;\blacksquare\; \forall_{\alpha\in A}\forall_{a\in\alpha}(a \in \beta_0)$

(1.7) $(\alpha \in A \wedge a \in \alpha) \iff a \in \gamma \;\blacksquare\; \forall_{a\in\gamma}(a \in \beta_0) \;\blacksquare\; \gamma \subseteq \beta_0$

(1.8) $\beta_0 \subset \mathbb{Q} \;\blacksquare\; \gamma \subseteq \beta_0 \subset \mathbb{Q} \;\blacksquare\; \gamma \subset \mathbb{Q}$

(1.9) $\emptyset \neq \gamma \subset \mathbb{Q} \;\blacksquare\; \mathit{CutI}[\gamma]$

(1.10) $(p \in \gamma \wedge q \in \mathbb{Q} \wedge q < p) \implies \ldots$

(1.10.1) $p \in \gamma \;\blacksquare\; \exists_{\alpha\in A}(p \in \alpha) \;\blacksquare\; \alpha_1 := choice(\{\alpha \in A : p \in \alpha\})$

(1.10.2) $p \in \alpha_1 \wedge q \in \mathbb{Q} \wedge q < p \;\blacksquare\; q \in \alpha_1 \;\blacksquare\; q \in \gamma$

(1.11) $(p \in \gamma \wedge q \in \mathbb{Q} \wedge q < p) \implies q \in \gamma \;\blacksquare\; \forall_{p\in\gamma}\forall_{q\in\mathbb{Q}}(q < p \implies q \in \gamma) \;\blacksquare\; \mathit{CutII}[\gamma]$

(1.12) $p \in \gamma \implies \ldots$

(1.12.1) $\exists_{\alpha\in A}(p \in \alpha) \;\blacksquare\; \alpha_2 := choice(\{\alpha \in A : p \in \alpha\})$

(1.12.2) $\alpha_2 \in \mathbb{R} \;\blacksquare\; \mathit{CutII}[\alpha_2] \;\blacksquare\; \exists_{r\in\alpha_2}(p < r) \;\blacksquare\; r_0 := choice(\{r \in \alpha_2 : p < r\})$

(1.12.3) $r_0 \in \alpha_2 \;\blacksquare\; r_0 \in \gamma$

(1.12.4) $p < r_0 \;\blacksquare\; p < r_0 \wedge r_0 \in \gamma \;\blacksquare\; \exists_{r\in\gamma}(p < r)$

(1.13) $p \in \gamma \implies \exists_{r\in\gamma}(p < r) \;\blacksquare\; \forall_{p\in\gamma}\exists_{r\in\gamma}(p < r) \;\blacksquare\; \mathit{CutIII}[\gamma]$

(1.14) $\mathit{CutI}[\gamma] \wedge \mathit{CutII}[\gamma] \wedge \mathit{CutIII}[\gamma] \;\blacksquare\; \gamma \in \mathbb{R}$

(1.15) $\forall_{\alpha\in A}(\alpha \subseteq \gamma) \;\blacksquare\; \forall_{\alpha\in A}(\alpha \leq_{\mathbb{R}} \gamma)$

(1.16) $\forall_{\alpha\in A}(\alpha \leq_{\mathbb{R}} \gamma) \wedge \gamma \in \mathbb{R} \;\blacksquare\; \mathit{UpperBound}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}]$

(1.17) $\delta <_{\mathbb{R}} \gamma \implies \ldots$

(1.17.1) $\delta \subset \gamma \;\blacksquare\; \exists_s(s \in \gamma \wedge s \notin \delta) \;\blacksquare\; s_0 := choice(\{s \in \mathbb{Q} : s \in \gamma \wedge s \notin \delta\})$

(1.17.2) $s_0 \in \gamma \;\blacksquare\; \exists_{\alpha\in A}(s_0 \in \alpha) \;\blacksquare\; \alpha_3 := choice(\{\alpha \in A : s_0 \in \alpha\})$

(1.17.3) $s_0 \in \alpha_3 \wedge s_0 \notin \delta \;\blacksquare\; \exists_{s\in\mathbb{Q}}(s \in \alpha_3 \wedge s \notin \delta)$

(1.17.4) $\delta \geq_{\mathbb{R}} \alpha_3 \implies \ldots$

(1.17.4.1) $\alpha_3 \subseteq \delta \;\blacksquare\; \forall_{s\in\mathbb{Q}}(s \in \alpha_3 \implies s \in \delta) \;\blacksquare\; \neg\exists_{s\in\mathbb{Q}}(s \in \alpha_3 \wedge s \notin \delta)$

(1.17.4.2) $\neg\exists_{s\in\mathbb{Q}}(s \in \alpha_3 \wedge s \notin \delta) \wedge \exists_{s\in\mathbb{Q}}(s \in \alpha_3 \wedge s \notin \delta) \;\blacksquare\; \bot$

(1.17.5) $\delta \geq_{\mathbb{R}} \alpha_3 \implies \bot \;\blacksquare\; \delta <_{\mathbb{R}} \alpha_3 \;\blacksquare\; \exists_{\alpha\in A}(\delta <_{\mathbb{R}} \alpha) \;\blacksquare\; \exists_{\alpha\in A}\big(\neg(\alpha \leq_{\mathbb{R}} \delta)\big)$

(1.17.6) $\neg\forall_{\alpha\in A}(\alpha \leq_{\mathbb{R}} \delta) \;\blacksquare\; \neg\mathit{UpperBound}[\delta, A, \mathbb{R}, <_{\mathbb{R}}]$

(1.18) $\delta <_{\mathbb{R}} \gamma \implies \neg\mathit{UpperBound}[\delta, A, \mathbb{R}, <_{\mathbb{R}}]) \;\blacksquare\; \forall_{\delta}(\delta <_{\mathbb{R}} \gamma \implies \neg\mathit{UpperBound}[\delta, A, \mathbb{R}, <_{\mathbb{R}}])$

(1.19) $\mathit{UpperBound}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}] \wedge \forall_{\delta}(\delta <_{\mathbb{R}} \gamma \implies \neg\mathit{UpperBound}[\delta, A, \mathbb{R}, <_{\mathbb{R}}])$

(1.20) $\mathit{LUB}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}] \;\blacksquare\; \exists_{\gamma\in S}(\mathit{LUB}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}])$

(2) $(\emptyset \neq A \subset \mathbb{R} \wedge \mathit{BoundedAbove}[A, \mathbb{R}, <_{\mathbb{R}}]) \implies \exists_{\gamma\in S}(\mathit{LUB}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}])$

(3) $\forall_A\Big((\emptyset \neq A \subset \mathbb{R} \wedge \mathit{BoundedAbove}[A, \mathbb{R}, <_{\mathbb{R}}]) \implies \exists_{\gamma\in S}(\mathit{LUB}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}])\Big) \;\blacksquare\; \mathit{LUBProperty}[\mathbb{R}, <_{\mathbb{R}}]$

$+_{\mathbb{R}}[\alpha, \beta] := \alpha, \beta \in \mathbb{R} \wedge (\alpha +_{\mathbb{R}} \beta) = \{r + s : r \in \alpha \wedge s \in \beta\}$

$0_{\mathbb{R}} := \{x \in \mathbb{Q} : x < 0\}$

$\mathit{ZeroInR} := 0_{\mathbb{R}} \in \mathbb{R}$

(1) $-1 \in 0_{\mathbb{R}} \wedge 1 \notin 0_{\mathbb{R}} \;\blacksquare\; \emptyset \neq 0_{\mathbb{R}} \subseteq \mathbb{Q} \;\blacksquare\; \mathit{CutI}[0_{\mathbb{R}}]$

(2) $(x \in 0_{\mathbb{R}} \wedge y \in \mathbb{Q} \wedge y < x) \implies y < x < 0 \implies y < 0 \implies y \in 0_{\mathbb{R}} \;\blacksquare\; \forall_{x\in 0_{\mathbb{R}}}\forall_{y\in\mathbb{Q}}(y_0 < x \implies y \in 0_{\mathbb{R}}) \;\blacksquare\; \mathit{CutII}[0_{\mathbb{R}}]$

(3) $y := x/2 \;\blacksquare\; (x \in 0_{\mathbb{R}}) \implies (x < y < 0) \implies \exists_{y\in 0_{\mathbb{R}}}(x < y) \;\blacksquare\; \forall_{x\in 0_{\mathbb{R}}}\exists_{y\in 0_{\mathbb{R}}}(x < y) \;\blacksquare\; \mathit{CutIII}[0_{\mathbb{R}}]$

(4) $\mathit{CutI}[0_{\mathbb{R}}] \wedge \mathit{CutII}[0_{\mathbb{R}}] \wedge \mathit{CutIII}[0_{\mathbb{R}}] \;\blacksquare\; 0_{\mathbb{R}} \in \mathbb{R}$

$\mathit{FieldAdditionClosureOfR} := (\alpha, \beta \in \mathbb{R}) \implies \big((\alpha +_{\mathbb{R}} \beta) \in \mathbb{R}\big)$

(1) $(\alpha, \beta \in \mathbb{R}) \implies \ldots$

(1.1) $(\alpha +_{\mathbb{R}} \beta) = \{r + s : r \in \alpha \wedge s \in \beta\}$

(1.2) $\emptyset \neq \alpha \subset \mathbb{Q} \wedge \emptyset \neq \beta \subset \mathbb{Q}$

(1.3) $\exists_a(a \in \alpha)\,;\exists_b(b \in \beta) \;\blacksquare\; a_0 := choice(\{a : a \in \alpha\})\,; b_0 := choice(\{b : b \in \beta\}) \;\blacksquare\; a_0 + b_0 \in \alpha +_{\mathbb{R}} \beta$

(1.4) $\exists_x(x \notin \alpha)\,;\exists_y(y_0 \notin \beta) \;\blacksquare\; x_0 := choice(\{x : x \notin \alpha\})\,; y_0 := choice(\{y : y \notin \beta\})$

(1.5) $\forall_{r\in\alpha}(r < x_0)\,;\forall_{s\in\beta}(s < y_0) \;\blacksquare\; \forall_{r\in\alpha}\forall_{s\in\beta}(r + s < x_0 + y_0) \;\blacksquare\; x_0 + y_0 \notin \alpha +_{\mathbb{R}} \beta$

(1.6) $\emptyset \neq \alpha +_{\mathbb{R}} \beta \subset \mathbb{Q} \;\blacksquare\; \mathit{CutI}[\alpha +_{\mathbb{R}} \beta]$

(1.7) $(p \in \alpha +_{\mathbb{R}} \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies \ldots$

(1.7.1) $\exists_{r\in\alpha}\exists_{s\in\beta}(p = r + s) \;\blacksquare\; (r_0, s_0) := choice\big((r, s) \in \alpha \times \beta : p = r + s\big)$

(1.7.2) $q < p = r_0 + s_0 \;\blacksquare\; (q - s_0) < r_0 \;\blacksquare\; (q - s_0) \in \alpha$

(1.7.3) $s_0 \in \beta \;\blacksquare\; q = (q - s_0) + s_0 \in \alpha +_{\mathbb{R}} \beta \;\blacksquare\; q \in \alpha +_{\mathbb{R}} \beta$

(1.8) $(p \in \alpha +_{\mathbb{R}} \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies q \in \alpha +_{\mathbb{R}} \beta \;\blacksquare\; \forall_{p\in\alpha+_{\mathbb{R}}\beta}\forall_{q\in\mathbb{Q}}(q < p \implies q \in \alpha +_{\mathbb{R}} \beta) \;\blacksquare\; \mathit{CutII}[\alpha +_{\mathbb{R}} \beta]$

(1.9) $p \in \alpha \implies \ldots$

(1.9.1) $\exists_{r\in\alpha}\exists_{s\in\beta}(p = r + s) \;\blacksquare\; (r_1, s_1) := choice\big(\{(r, s) \in \alpha \times \beta : p = r + s\}\big)$

(1.9.2) $r_1 \in \alpha \;\blacksquare\; \exists_{t\in\alpha}(r_1 < t) \;\blacksquare\; t_0 := choice(\{t \in \alpha : r_1 < t\})$

(1.9.3) $s_1 \in \beta \;\blacksquare\; t + s_1 \in \alpha +_{\mathbb{R}} \beta \wedge p = r_1 + s_1 < t + s_1 \;\blacksquare\; \exists_{r\in\alpha+_{\mathbb{R}}\beta}(p < r)$

(1.10) $p \in \alpha \implies \exists_{r\in\alpha+_{\mathbb{R}}\beta}(p < r) \;\blacksquare\; \forall_{p\in\alpha+_{\mathbb{R}}\beta}\exists_{r\in\alpha+_{\mathbb{R}}\beta}(p < r) \;\blacksquare\; \mathit{CutIII}[\alpha +_{\mathbb{R}} \beta]$

(1.11) $\mathit{CutI}[\alpha +_{\mathbb{R}} \beta] \wedge \mathit{CutII}[\alpha +_{\mathbb{R}} \beta] \wedge \mathit{CutIII}[\alpha +_{\mathbb{R}} \beta] \;\blacksquare\; \alpha +_{\mathbb{R}} \beta \in \mathbb{R}$

(2) $(\alpha, \beta \in \mathbb{R}) \implies \big((\alpha +_{\mathbb{R}} \beta) \in \mathbb{R}\big)$

$\mathit{FieldAdditionCommutativityOfR} := (\alpha, \beta \in \mathbb{R}) \implies (\alpha +_{\mathbb{R}} \beta = \beta +_{\mathbb{R}} \alpha)$

(1) $\alpha +_{\mathbb{R}} \beta = \{r + s : r \in \alpha \wedge s \in \beta\} = \{s + r : s \in \beta \wedge r \in \alpha\} = \beta +_{\mathbb{R}} \alpha$

$\mathit{FieldAdditionAssociativityOfR} := (\alpha, \beta, \gamma \in \mathbb{R}) \implies \big((\alpha +_{\mathbb{R}} \beta) +_{\mathbb{R}} \gamma = \alpha +_{\mathbb{R}} (\beta +_{\mathbb{R}} \gamma)\big)$

(1) $(\alpha, \beta, \gamma \in \mathbb{R}) \implies \ldots$

(1.1) $(\alpha +_{\mathbb{R}} \beta) +_{\mathbb{R}} \gamma = \{(a + b) + c : a \in \alpha \wedge b \in \beta \wedge c \in \gamma\} = \ldots$

(1.2) $\{a + (b + c) : a \in \alpha \wedge b \in \beta \wedge c \in \gamma\} = \alpha +_{\mathbb{R}} (\beta +_{\mathbb{R}} \gamma)$

(2) $(\alpha, \beta, \gamma \in \mathbb{R}) \implies (\alpha +_{\mathbb{R}} \beta) +_{\mathbb{R}} \gamma = \alpha +_{\mathbb{R}} (\beta +_{\mathbb{R}} \gamma)$

$\mathit{FieldAdditionIdentityOfR} := (\alpha \in \mathbb{R}) \implies 0_{\mathbb{R}} +_{\mathbb{R}} \alpha = \alpha$

(1) $\alpha \in \mathbb{R} \implies \ldots$

(1.1) $(r \in \alpha \wedge s \in 0_{\mathbb{R}}) \implies \ldots$

(1.1.1) $s < 0 \;\blacksquare\; r + s < r + 0 = r \;\blacksquare\; r + s < r \;\blacksquare\; r + s \in \alpha$

(1.2) $(r \in \alpha \wedge s \in 0_{\mathbb{R}}) \implies r + s \in \alpha \;\blacksquare\; \forall_{r\in\alpha}\forall_{s\in 0_{\mathbb{R}}}(r + s \in \alpha)$

(1.3) $(r \in \alpha \wedge s \in 0_{\mathbb{R}}) \iff (r + s \in \alpha +_{\mathbb{R}} 0_{\mathbb{R}}) \;\blacksquare\; \forall_{p\in\alpha+_{\mathbb{R}}0_{\mathbb{R}}}(p \in \alpha) \;\blacksquare\; \alpha +_{\mathbb{R}} 0_{\mathbb{R}} \subseteq \alpha$

(1.4) $p \in \alpha \implies \ldots$

(1.4.1) $\exists_{r\in\alpha}(p < r) \;\blacksquare\; r_2 := choice(\{r \in \alpha : p < r\})$

(1.4.2) $p < r_2 \;\blacksquare\; p - r_2 < r_2 - r_2 = 0 \;\blacksquare\; (p - r_2) < 0 \;\blacksquare\; (p - r_2) \in 0_{\mathbb{R}}$

(1.4.3) $r_2 \in \alpha \;\blacksquare\; p = r_2 + (p - r_2) \in \alpha +_{\mathbb{R}} 0_{\mathbb{R}} \;\blacksquare\; p \in \alpha +_{\mathbb{R}} 0_{\mathbb{R}}$

(1.5) $p \in \alpha \implies p \in \alpha +_{\mathbb{R}} 0_{\mathbb{R}} \;\blacksquare\; \forall_{p\in\alpha}(p \in \alpha +_{\mathbb{R}} 0_{\mathbb{R}}) \;\blacksquare\; \alpha \subseteq \alpha +_{\mathbb{R}} 0_{\mathbb{R}}$

(1.6) $\alpha +_{\mathbb{R}} 0_{\mathbb{R}} \subseteq \alpha \wedge \alpha \subseteq \alpha +_{\mathbb{R}} 0_{\mathbb{R}} \;\blacksquare\; 0_{\mathbb{R}} +_{\mathbb{R}} \alpha = \alpha$

(2) $\alpha \in \mathbb{R} \implies 0_{\mathbb{R}} +_{\mathbb{R}} \alpha = \alpha$

$\mathit{FieldAdditionInverseOfR} := (\alpha \in \mathbb{R}) \implies \exists_{-\alpha\in\mathbb{R}}\big(\alpha +_{\mathbb{R}} (-\alpha) = 0_{\mathbb{R}}\big)$

(1) $\alpha \in \mathbb{R} \implies \ldots$

(1.1) $\beta := \{p \in \mathbb{Q} : \exists_{r>0}(-p - r \notin \alpha)\}$

(1.2) $\alpha \subset \mathbb{Q} \;\blacksquare\; \exists_{s\in\mathbb{Q}}(s \notin \alpha) \;\blacksquare\; s_0 := choice(\{s : s \notin \alpha\}) \;\blacksquare\; p_0 := -s_0 - 1$

(1.3) $-p_0 - 1 = -(-s_0 - 1) - 1 = s_0 \notin \alpha \;\blacksquare\; -p_0 - 1 \notin \alpha \;\blacksquare\; \exists_{r>0}(-p_0 - r \notin \alpha) \;\blacksquare\; p_0 \in \beta$

(1.4) $\emptyset \neq \alpha \;\blacksquare\; \exists_{q\in\alpha} \;\blacksquare\; q_0 := choice(\{q \in \mathbb{Q} : q \in \alpha\})$

(1.5) $r > 0 \implies \ldots$

(1.5.1) $q_0 \in \alpha \;\blacksquare\; -(-q_0) - r = q_0 - r < q_0 \;\blacksquare\; -(-q_0) - r < q_0 \;\blacksquare\; -(-q_0) - r \in \alpha$

(1.6) $\forall_{r>0}\big(-(-q_0) - r \in \alpha\big) \;\blacksquare\; \neg\exists_{r>0}\big(-(-q_0) - r \notin \alpha\big) \;\blacksquare\; -q_0 \notin \beta$

(1.7) $\emptyset \neq \beta \subset \mathbb{Q} \;\blacksquare\; \mathit{CutI}[\beta]$

(1.8) $(p \in \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies \ldots$

(1.8.1) $p \in \beta \ \blacksquare\ \exists_{r>0}(-p - r \notin \alpha) \ \blacksquare\ r_0 := choice(\{r > 0 : -p - r \notin \alpha\})$

(1.8.2) $q < p \ \blacksquare\ -p - r < -q - r$

(1.8.3) $-q - r \notin \alpha \ \blacksquare\ q \in \beta$

(1.9) $(p \in \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies q \in \beta \ \blacksquare\ \forall_{p\in\beta}\forall_{q\in\mathbb{Q}}(q < p \implies q \in \beta) \ \blacksquare\ CutII[\beta]$

(1.10) $p \in \beta \implies \ldots$

(1.10.1) $p \in \beta \ \blacksquare\ \exists_{r>0}(-p - r \notin \alpha) \ \blacksquare\ r_1 := choice(\{r > 0 : -p - r \notin \alpha\})$

(1.10.2) $t_0 := p + (r_1/2)$

(1.10.3) $r_1 > 0 \ \blacksquare\ r_1/2 > 0$

(1.10.4) $t_0 > t_0 - (r_1/2) = p \ \blacksquare\ t_0 > p$

(1.10.5) $-t_0 - (r_1/2) = -\big(p + (r_1/2)\big) - (r_1/2) = -p - r_1$

(1.10.6) $-p - r_1 \notin \alpha \ \blacksquare\ -t_0 - (r_1/2) \notin \alpha \ \blacksquare\ \exists_{r>0}(-t_0 - r \notin \alpha) \ \blacksquare\ t_0 \in \beta$

(1.10.7) $t_0 > p \wedge t_0 \in \beta \ \blacksquare\ \exists_{t\in\beta}(p < t)$

(1.11) $p \in \beta \implies \exists_{t\in\beta}(p < t) \ \blacksquare\ \forall_{p\in\beta}\exists_{t\in\beta}(p < t) \ \blacksquare\ CutIII[\beta]$

(1.12) $CutI[\beta] \wedge CutII[\beta] \wedge CutIII[\beta] \ \blacksquare\ \beta \in \mathbb{R}$

(1.13) $(r \in \alpha \wedge s \in \beta) \implies \ldots$

(1.13.1) $s \in \beta \ \blacksquare\ \exists_{t>0}(-s - t \notin \alpha) \ \blacksquare\ t_1 := choice(\{t > 0 : -s - t \notin \alpha\}) \ \blacksquare\ -s - t_1 < -s$

(1.13.2) $\alpha \in \mathbb{R} \wedge s, t_1 \in \mathbb{Q} \wedge -s - t_1 < -s \wedge -s - t_1 \notin \alpha \ \blacksquare\ -s \notin \alpha$

(1.13.3) $\alpha \in \mathbb{R} \wedge r \in \alpha \wedge -s \notin \alpha \ \blacksquare\ r < -s \ \blacksquare\ r + s < 0 \ \blacksquare\ r + s \in 0_\mathbb{R}$

(1.14) $(r \in \alpha \wedge s \in \beta) \implies r + s \in 0_\mathbb{R} \ \blacksquare\ \forall_{(r,s)\in\alpha\times\beta}(r + s \in 0_\mathbb{R}) \ \blacksquare\ \alpha +_\mathbb{R} \beta \subseteq 0_\mathbb{R}$

(1.15) $v \in 0_\mathbb{R} \implies \ldots$

(1.15.1) $v < 0 \ \blacksquare\ w_0 := -v/2 \ \blacksquare\ w > 0$

(1.15.2) $\exists_{n\in\mathbb{Z}}\big(nw_0 \in \alpha \wedge (n+1)w_0 \notin \alpha\big) \ \blacksquare\ n_0 := choice\big(\{n \in \mathbb{Z} : nw_0 \in \alpha \wedge (n+1)w_0 \notin \alpha\}\big)$ from: $ARCHIMEDEANPROPERTYOFQ + LUB$???

(1.15.3) $p_0 := -(n_0 + 2)w_0 \ \blacksquare\ -p_0 - w_0 = (n_0 + 2)w_0 - w_0 = (n_0 + 1)w_0 \notin \alpha \ \blacksquare\ -p_0 - w_0 \notin \alpha \ \blacksquare\ p_0 \in \beta$

(1.15.4) $n_0 w_0 \in \alpha \wedge p_0 \in \beta \ \blacksquare\ n_0 w_0 + p_0 = n_0(-v/2) + -(n_0 + 2) - v/2 = v \in \alpha +_\mathbb{R} \beta$

(1.16) $v \in 0_\mathbb{R} \implies v \in \alpha +_\mathbb{R} \beta \ \blacksquare\ \forall_{v\in 0_\mathbb{R}}(v \in \alpha +_\mathbb{R} \beta) \ \blacksquare\ 0_\mathbb{R} \subseteq \alpha +_\mathbb{R} \beta$

(1.17) $\alpha +_\mathbb{R} \beta \subseteq 0_\mathbb{R} \wedge 0_\mathbb{R} \subseteq \alpha +_\mathbb{R} \beta \ \blacksquare\ \alpha +_\mathbb{R} \beta = 0_\mathbb{R}$

(1.18) $\beta \in \mathbb{R} \wedge \alpha +_\mathbb{R} \beta = 0_\mathbb{R} \ \blacksquare\ \exists_{-\alpha\in\mathbb{R}}\big(\alpha +_\mathbb{R} (-\alpha) = 0_\mathbb{R}\big)$

(2) $\alpha \in \mathbb{R} \implies \exists_{-\alpha\in\mathbb{R}}\big(\alpha +_\mathbb{R} (-\alpha) = 0_\mathbb{R}\big)$

$*_\mathbb{R}[\alpha, \beta] :=$ —

$1_\mathbb{R} := \{x \in \mathbb{Q} : x < 1\}$

$1IsNot0 := 0_\mathbb{R} \neq 1_\mathbb{R}$ —

$1InR := 1_\mathbb{R} \in \mathbb{R}$ —

$FieldMultiplicationClosureOfR := (\alpha, \beta \in \mathbb{R}) \implies \big((\alpha *_\mathbb{R} \beta) \in \mathbb{R}\big)$ —

$FieldMultiplicationCommutativityOfR := (\alpha, \beta \in \mathbb{R}) \implies (\alpha *_\mathbb{R} \beta = \beta *_\mathbb{R} \alpha)$ —

$FieldMultiplicationAssociativityOfR := (\alpha, \beta, \gamma \in \mathbb{R}) \implies \big((\alpha *_\mathbb{R} \beta) *_\mathbb{R} \gamma = \alpha *_\mathbb{R} (\beta *_\mathbb{R} \gamma)\big)$ —

$FieldMultiplicationIdentityOfR := (\alpha \in \mathbb{R}) \implies 1_\mathbb{R} *_\mathbb{R} \alpha = \alpha$ —

$FieldMultiplicationInverseOfR := (\alpha \in \mathbb{R}) \implies \exists_{1/\alpha\in\mathbb{R}}\big(\alpha *_\mathbb{R} (1/\alpha) = 1_\mathbb{R}\big)$ —

$FieldDistributativityOfR := (\alpha, \beta, \gamma \in \mathbb{R}) \implies \gamma *_\mathbb{R} (\alpha +_\mathbb{R} \beta) = \gamma *_\mathbb{R} \alpha + \gamma *_\mathbb{R} \beta$ —

$FieldWithR := Field[\mathbb{R}, +_\mathbb{R}, *_\mathbb{R}]$ —

$OrderedFieldWithR := OrderedField[\mathbb{R}, +_\mathbb{R}, *_\mathbb{R}, <_\mathbb{R}]$ —

$\mathbb{Q}_\mathbb{R} := \{\{r \in \mathbb{Q} : r < q\} : q \in \mathbb{Q}\}$

$QROrderedSubfieldOfR := OrderedSubfield[\mathbb{Q}_\mathbb{R}, \mathbb{R}, +_\mathbb{R}, *_\mathbb{R}, <_\mathbb{R}]$ —

$QIsomorphicToQR := \mathbb{Q}_\mathbb{R} \simeq \mathbb{Q}$ —

$CompletenessOfR := \exists_\mathbb{R}(LUBProperty[\mathbb{R}, <_\mathbb{R}] \wedge OrderedSubfield[\mathbb{Q}, \mathbb{R}, +_\mathbb{R}, *_\mathbb{R}, <_\mathbb{R}])$ —

(1.20)

$ArchimedeanPropertyOfR := \forall_{x,y\in\mathbb{R}}\big(x > 0 \implies \exists_{n\in\mathbb{N}^+}(nx > y)\big)$

(1) $(x, y \in \mathbb{R} \wedge x > 0) \implies \ldots$

(1.1) $A := \{nx : n \in \mathbb{N}^+\} \blacksquare (\emptyset \neq A \subset \mathbb{R}) \wedge \big(a \in A \iff \exists_{m \in \mathbb{N}^+}(mx = a)\big)$

(1.2) $\neg\exists_{n \in \mathbb{N}^+}(nx > y) \implies \ldots$

(1.2.1) $\neg\exists_{n \in \mathbb{N}^+}(nx > y) \blacksquare \forall_{n \in \mathbb{N}^+}(nx \leq y) \blacksquare \mathit{UpperBound}[y_0, A, \mathbb{R}, <] \blacksquare \mathit{BoundedAbove}[A, \mathbb{R}, <]$

(1.2.2) $\mathit{CompletenessOfR} \blacksquare \mathit{LUBProperty}[\mathbb{R}, <]$

(1.2.3) $(\mathit{LUBProperty}[\mathbb{R}, <]) \wedge (\emptyset \neq A \subset \mathbb{R}) \wedge (\mathit{BoundedAbove}[A, \mathbb{R}, <]) \blacksquare \exists_{\alpha \in \mathbb{R}}(\mathit{LUB}[\alpha, A, \mathbb{R}, <]) \ \ldots$

(1.2.4) $\ldots \alpha_0 := \mathit{choice}(\{\alpha \in \mathbb{R} : \mathit{LUB}[\alpha, A, \mathbb{R}, <]\}) \blacksquare \mathit{LUB}[\alpha_0, A, \mathbb{R}, <]$

(1.2.5) $x > 0 \blacksquare \alpha_0 - x < \alpha_0$

(1.2.6) $(\alpha_0 - x < \alpha_0) \wedge (\mathit{LUB}[\alpha_0, A, \mathbb{R}, <]) \blacksquare \neg\mathit{UpperBound}[\alpha_0 - x, A, \mathbb{R}, <]$

(1.2.7) $\neg\mathit{UpperBound}[\alpha_0 - x, A, \mathbb{R}, <] \blacksquare \exists_{c \in A}(\alpha_0 - x < c) \ \ldots$

(1.2.8) $\ldots c_0 := \mathit{choice}(\{c \in A : \alpha_0 - x < c\}) \blacksquare (c_0 \in A) \wedge (\alpha_0 - x < c_0)$

(1.2.9) $(c_0 \in A) \wedge \big(a \in A \iff \exists_{m \in \mathbb{N}^+}(mx = a)\big) \blacksquare \exists_{m \in \mathbb{N}^+}(mx = c_0) \ \ldots$

(1.2.10) $\ldots m_0 := \mathit{choice}(\{m \in \mathbb{N}^+ : mx = c_0\}) \blacksquare (m_0 \in \mathbb{N}^+) \wedge (m_0 x = c_0)$

(1.2.11) $(\alpha_0 - x < c_0) \wedge (m_0 x = c_0) \blacksquare \alpha_0 - x < c_0 = m_0 x \blacksquare \alpha_0 < m_0 x + x \blacksquare \alpha_0 < (m_0 + 1)x$

(1.2.12) $m_0 \in \mathbb{N}^+ \blacksquare m_0 + 1 \in \mathbb{N}^+$

(1.2.13) $(m_0 + 1 \in \mathbb{N}^+) \wedge \big(a \in A \iff \exists_{m \in \mathbb{N}^+}(mx = a)\big) \blacksquare (m_0 + 1)x \in A$

(1.2.14) $\big(\alpha_0 < (m_0 + 1)x\big) \wedge \big((m_0 + 1)x \in A\big) \blacksquare \exists_{c \in A}(\alpha_0 < c)$

(1.2.15) $\mathit{LUB}[\alpha_0, A, \mathbb{R}, <] \blacksquare \mathit{UpperBound}[\alpha_0, A, \mathbb{R}, <] \blacksquare \forall_{c \in A}(c \leq \alpha_0) \blacksquare \neg\exists_{c \in A}(c > \alpha_0) \blacksquare \neg\exists_{c \in A}(\alpha_0 < c)$

(1.2.16) $\big(\exists_{c \in A}(\alpha_0 < c)\big) \wedge \big(\neg\exists_{c \in A}(\alpha_0 < c)\big) \blacksquare \perp$

(1.3) $\neg\exists_{n \in \mathbb{N}^+}(nx > y) \implies \perp \blacksquare \exists_{n \in \mathbb{N}^+}(nx > y)$

(2) $(x, y \in \mathbb{R} \wedge x > 0) \implies \exists_{n \in \mathbb{N}^+}(nx > y) \blacksquare \forall_{x,y \in \mathbb{R}}\big(x > 0 \implies \exists_{n \in \mathbb{N}^+}(nx > y)\big)$

$\mathit{QDenseInR} := \forall_{x,y \in \mathbb{R}}\Big(x < y \implies \exists_{p \in \mathbb{Q}}(x < p < y)\Big)$

(1) $(x, y \in \mathbb{R} \wedge x < y) \implies \ldots$

(1.1) $x < y \blacksquare (0 < y - x) \wedge (y - x \in \mathbb{R})$

(1.2) $\mathit{ArchimedeanPropertyOfR} \wedge (0 < y - x) \wedge (y - x, 1 \in \mathbb{R}) \blacksquare \exists_{n \in \mathbb{N}^+}\big(n(y - x) > 1\big) \ \ldots$

(1.3) $\ldots n_0 := \mathit{choice}\big(\{n \in \mathbb{N}^+ : n(y - x) > 1\}\big) \blacksquare (n_0 \in \mathbb{N}^+) \wedge \big(n_0(y - x) > 1\big)$

(1.4) $(n_0 \in \mathbb{N}^+) \wedge (x \in \mathbb{R}) \blacksquare n_0 x, -n_0 x \in \mathbb{R}$

(1.5) $\mathit{ArchimedeanPropertyOfR} \wedge (1 > 0) \wedge (n_0 x, 1 \in \mathbb{R}) \blacksquare \exists_{m \in \mathbb{N}^+}\big(m(1) > n_0 x\big) \ \ldots$

(1.6) $\ldots m_1 := \mathit{choice}\big(\{m \in \mathbb{N}^+ : m(1) > n_0 x\}\big) \blacksquare (m_1 \in \mathbb{N}^+) \wedge (m_1 > n_0 x)$

(1.7) $\mathit{ArchimedeanPropertyOfR} \wedge (1 > 0) \wedge (-n_0 x, 1 \in \mathbb{R}) \blacksquare \exists_{m \in \mathbb{N}^+}\big(m(1) > -n_0 x\big) \ \ldots$

(1.8) $\ldots m_2 := \mathit{choice}\big(\{m \in \mathbb{N}^+ : m(1) > -n_0 x\}\big) \blacksquare (m_2 \in \mathbb{N}^+) \wedge (m_2 > -n_0 x)$

(1.9) $(m_1 > n_0 x) \wedge (m_2 > -n_0 x) \blacksquare -m_2 < n_0 x < m_1$

(1.10) $m_1, m_2 \in \mathbb{N}^+ \blacksquare |m_1 - (-m_2)| \geq 2$

(1.11) $(-m_2 < n_0 x < m_1) \wedge \big(|m_1 - (-m_2)| \geq 2\big) \blacksquare \exists_{m \in \mathbb{Z}}\big((-m_2 < m < m_1) \wedge (m - 1 \leq n_0 x < m)\big) \ \ldots$

(1.12) $\ldots m_0 := \mathit{choice}\big(\{m \in \mathbb{Z} : (-m_2 < m < m_1) \wedge (m - 1 \leq n_0 x < m)\}\big) \blacksquare (-m_2 < m_0 < m_1) \wedge (m_0 - 1 \leq n_0 x < m_0)$

(1.13) $\big(n_0(y - x) > 1\big) \wedge (m_0 - 1 \leq n_0 x < m_0) \blacksquare n_0 x < m_0 \leq 1 + n_0 x < n_0 y \blacksquare n_0 x < m_0 < n_0 y$

(1.14) $(n_0 \in \mathbb{N}^+) \wedge (n_0 x < m_0 < n_0 y) \blacksquare x < m_0/n_0 < y$

(1.15) $m_0, n_0 \in \mathbb{Z} \blacksquare m_0/n_0 \in \mathbb{Q}$

(1.16) $(m_0/n_0 \in \mathbb{Q}) \wedge (x < m_0/n_0 < y) \blacksquare \exists_{p \in \mathbb{Q}}(x < p < y)$

(2) $(x, y \in \mathbb{R} \wedge x < y) \implies \exists_{p \in \mathbb{Q}}(x < p < y) \blacksquare \forall_{x,y \in \mathbb{R}}\Big(x < y \implies \exists_{p \in \mathbb{Q}}(x < p < y)\Big)$

(1.21)

$\mathit{RootLemma} := (0 < a < b) \implies \Big(b^n - a^n \leq (b - a)nb^{n-1}\Big)$

(1) $(0 < a < b) \implies \ldots$

(1.1) $b^n - a^n = (b - a)\sum_{i=1}^{n}(b^{n-i}a^{i-1})$

(1.2) $0 < a < b \blacksquare b/a > 1$

(1.3) $b/a > 1$ ▮ $\sum_{i=1}^{n}(b^{n-i}a^{i-1}) \leq \sum_{i=1}^{n}\left(b^{n-i}a^{i-1}(b/a)^{i-1}\right) = \sum_{i=1}^{n}(b^{n-1}) = nb^{n-1}$ ▮ $\sum_{i=1}^{n}(b^{n-i}a^{i-1}) \leq \sum_{i=1}^{n}(b^{n-1}) = nb^{n-1}$

(1.4) $b^n - a^n = (b-a)\sum_{i=1}^{n}(b^{n-i}a^{i-1}) \leq (b-a)nb^{n-1}$ ▮ $b^n - a^n \leq (b-a)nb^{n-1}$

(2) $(0 < a < b) \implies \left(b^n - a^n \leq (b-a)nb^{n-1}\right)$

$RootExistenceInR$ $:= \forall_{0<x\in\mathbb{R}}\forall_{0<n\in\mathbb{Z}}\exists!_{0<y\in\mathbb{R}}({y_0}^n = x)$

(1) $(0 < x \in \mathbb{R} \wedge 0 < n \in \mathbb{Z}) \implies \ldots$

(1.1) $E := \{t \in \mathbb{R} : t > 0 \wedge t^n < x\}$ ▮ $t \in E \iff (t \in \mathbb{R} \wedge t > 0 \wedge t^n < x)$

(1.2) $t_0 := x/(1+x)$ ▮ $\left(t_0 = x/(1+x)\right) \wedge (t_0 \in \mathbb{R})$

(1.3) $0 < x$ ▮ $0 < x < 1 + x$ ▮ $t_0 = x/(1+x) > 0$ ▮ $t_0 > 0$

(1.4) $1 = (1+x)/(1+x) > x/(1+x) = t_0$ ▮ $1 > t_0$

(1.5) $(t_0 > 0) \wedge (1 > t_0)$ ▮ $0 < t_0 < 1$

(1.6) $(0 < n \in \mathbb{Z}) \wedge (0 < t_0 < 1)$ ▮ ${t_0}^n \leq t_0$

(1.7) $0 < x$ ▮ $x > x/(1+x) = t_0$ ▮ $x > t_0$

(1.8) $({t_0}^n \leq t_0) \wedge (x > t_0)$ ▮ ${t_0}^n < x$

(1.9) $\left(t \in E \iff (t \in \mathbb{R} \wedge t > 0 \wedge t^n < x)\right) \wedge (t_0 \in \mathbb{R}) \wedge (t_0 > 0) \wedge ({t_0}^n < x)$ ▮ $t_0 \in E$ ▮ $\emptyset \neq E$

(1.10) $t_1 := choice(\{t \in \mathbb{R} : t > 1 + x\})$ ▮ $(t_1 \in \mathbb{R}) \wedge (t_1 > 1 + x)$

(1.11) $x > 0$ ▮ $t_1 > 1 + x > 1$ ▮ $t_1 > 1$ ▮ ${t_1}^n \geq t_1$

(1.12) $({t_1}^n \geq t_1) \wedge (t_1 > 1 + x) \wedge (1 > 0)$ ▮ ${t_1}^n \geq t_1 > 1 + x > x$ ▮ ${t_1}^n > x$

(1.13) $\left(t \in E \iff (t \in \mathbb{R} \wedge t > 0 \wedge t^n < x)\right) \wedge ({t_1}^n > x)$ ▮ $t_1 \notin E$ ▮ $E \subset \mathbb{R}$

(1.14) $(\emptyset \neq E) \wedge (E \subset \mathbb{R})$ ▮ $\emptyset \neq E \subset \mathbb{R}$

(1.15) $t \in E \implies \ldots$

(1.15.1) $(t \in E) \wedge \left(t \in E \iff (t \in \mathbb{R} \wedge t > 0 \wedge t^n < x)\right)$ ▮ $t^n < x$

(1.15.2) $({t_1}^n > x) \wedge (t^n < x)$ ▮ $t^n < x < {t_1}^n$ ▮ $t < t_1$

(1.16) $t \in E \implies t < t_1$ ▮ $\forall_{t\in E}(t \leq t_1)$ ▮ $UpperBound[t_1, E, \mathbb{R}, <]$ ▮ $BoundedAbove[E, \mathbb{R}, <]$

(1.17) $CompletenessOfR$ ▮ $LUBProperty[\mathbb{R}, <]$

(1.18) $(LUBProperty[\mathbb{R}, <]) \wedge (\emptyset \neq E \subset \mathbb{R}) \wedge (BoundedAbove[E, \mathbb{R}, <])$ ▮ $\exists_{y\in\mathbb{R}}(LUB[y, E, \mathbb{R}, <])$ ...

(1.19) ... $y_0 := choice(\{y \in \mathbb{R} : LUB[y, E, \mathbb{R}, <]\})$ ▮ $LUB[y_0, E, \mathbb{R}, <]$

(1.20) $(LUB[y_0, E, \mathbb{R}, <]) \wedge (t_0 \in E) \wedge (t_0 > 0)$ ▮ $0 < t_0 \leq y_0 \in \mathbb{R}$ ▮ $0 < y_0 \in \mathbb{R}$

(1.21) ${y_0}^n < x \implies \ldots$

(1.21.1) $k_0 := \frac{x - {y_0}^n}{n(y_0+1)^{n-1}}$ ▮ $k_0 \in \mathbb{R}$

(1.21.2) ${y_0}^n < x$ ▮ $0 < x - {y_0}^n$

(1.21.3) $(n > 0) \wedge (y_0 > 0)$ ▮ $0 < n(y_0 + 1)^{n-1}$

(1.21.4) $(0 < x - {y_0}^n) \wedge \left(0 < n(y_0+1)^{n-1}\right)$ ▮ $0 < \frac{x - {y_0}^n}{n(y_0+1)^{n-1}} = k_0$ ▮ $0 < k_0$

(1.21.5) $(0 < 1 \in \mathbb{R}) \wedge (0 < k_0 \in \mathbb{R})$ ▮ $0 < min(1, k_0) \in \mathbb{R}$

(1.21.6) $QDenseInR \wedge \left(0, min(1, k_0) \in \mathbb{R}\right) \wedge \left(0 < min(1, k_0)\right)$ ▮ $\exists_{h\in\mathbb{Q}}\left(0 < h < min(1, k_0)\right)$ ...

(1.21.7) ... $h_0 := choice\left(\{h \in \mathbb{Q} : 0 < h < min(1, k_0)\}\right)$ ▮ $(0 < h_0 < 1) \wedge \left(h_0 < k_0 = \frac{x - {y_0}^n}{n(y_0+1)^{n-1}}\right)$

(1.21.8) $(y_0 > 0) \wedge (h_0 > 0)$ ▮ $0 < y_0 < y_0 + h_0$

(1.21.9) $RootLemma \wedge (0 < y_0 < y_0 + h_0)$ ▮ $(y_0 + h_0)^n - {y_0}^n < h_0 n(y_0 + h_0)^{n-1}$

(1.21.10) $h_0 < 1$ ▮ $h_0 n(y_0 + h_0)^{n-1} < h_0 n(y_0 + 1)^{n-1}$

(1.21.11) $\left((y_0 + h_0)^n - {y_0}^n < h_0 n(y_0 + h_0)^{n-1}\right) \wedge \left(h_0 n(y_0 + h_0)^{n-1} < h_0 n(y_0 + 1)^{n-1}\right)$ ▮ $(y_0 + h_0)^n - {y_0}^n < h_0 n(y_0 + 1)^{n-1}$

(1.21.12) $\left(0 < n(y_0+1)^{n-1}\right) \wedge \left(h_0 < k_0 = \frac{x - {y_0}^n}{n(y_0+1)^{n-1}}\right)$ ▮ $h_0 n(y_0 + 1)^{n-1} < x - {y_0}^n$

(1.21.13) $\left((y_0 + h_0)^n - {y_0}^n < h_0 n(y_0 + 1)^{n-1}\right) \wedge \left(h_0 n(y_0 + 1)^{n-1} < x - {y_0}^n\right)$ ▮ $(y_0 + h_0)^n - {y_0}^n < x - {y_0}^n$ ▮ $(y_0 + h_0)^n < x$

(1.21.14) $(y_0 + h_0)^n - {y_0}^n < x - {y_0}^n$ ▮ $(y_0 + h_0)^n < x$

(1.21.15) $(0 < y_0\mathbb{R}) \wedge (0 < h_0 < \mathbb{R})$ ▮ $0 < y_0 < y_0 + h_0 \in \mathbb{R}$

(1.21.16) $\left(t \in E \iff (t \in \mathbb{R} \wedge t > 0 \wedge t^n < x)\right) \wedge \left((y_0 + h_0)^n < x\right) \wedge (0 < y_0 + h_0 \in \mathbb{R})$ ▮ $(y_0 + h_0)^n \in E$

(1.21.17) $\big((y_0+h_0)^n \in E\big) \wedge (y_0 < y_0 + h_0) \blacksquare \exists_{e\in E}(y_0 < e)$

(1.21.18) $LUB[y_0, E, \mathbb{R}, <] \blacksquare UpperBound[y_0, E, \mathbb{R}, <] \blacksquare \forall_{e\in E}(e \le y_0) \blacksquare \neg\exists_{e\in E}(e > y_0)$

(1.21.19) $\big(\exists_{e\in E}(e > y_0)\big) \wedge \big(\neg\exists_{e\in E}(e > y_0)\big) \blacksquare \bot$

(1.22) $y_0{}^n < x \implies \bot \blacksquare y_0{}^n \ge x$

(1.23) $y_0{}^n > x \implies \dots$

(1.23.1) $k_1 := \frac{y_0{}^n - x}{ny_0{}^{n-1}} \blacksquare (k_1 \in \mathbb{R}) \wedge (k_1 n y_0{}^{n-1} = y_0{}^n - x)$

(1.23.2) $(0 < x) \wedge (0 < n \in \mathbb{Z}) \blacksquare y_0{}^n - x < y_0{}^n \le ny_0{}^n \blacksquare y_0{}^n - x < ny_0{}^n$

(1.23.3) $y_0{}^n - x < ny_0{}^n \blacksquare k_1 = \frac{y_0{}^n - x}{ny_0{}^{n-1}} < \frac{ny_0{}^n}{ny_0{}^{n-1}} = y_0 \blacksquare k_1 < y_0$

(1.23.4) $y_0{}^n > x \blacksquare 0 < y_0{}^n - x$

(1.23.5) $(n > 0) \wedge (y_0 > 0) \blacksquare 0 < ny_0{}^{n-1}$

(1.23.6) $(0 < y_0{}^n - x) \wedge 0 < (ny_0{}^{n-1}) \blacksquare 0 < \frac{y_0{}^n - x}{ny_0{}^{n-1}} = k_1 \blacksquare 0 < k_1$

(1.23.7) $(k_1 < y_0) \wedge (0 < k_1) \blacksquare (0 < k_1 < y_0) \wedge (0 < y_0 - k_1 < y_0)$

(1.23.8) $t \ge y_0 - k_1 \implies \dots$

(1.23.8.1) $t \ge y_0 - k_1 \blacksquare t^n \ge (y_0 - k_1)^n \blacksquare -t^n \le -(y_0 - k_1)^n \blacksquare y_0{}^n - t^n \le y_0{}^n - (y_0 - k_1)^n$

(1.23.8.2) $RootLemma \wedge (0 < y_0 - k_1 < y_0) \blacksquare y_0{}^n - (y_0 - k_1)^n < k_1 n y_0{}^{n-1}$

(1.23.8.3) $\big(y_0{}^n - t^n \le y_0{}^n - (y_0 - k_1)^n\big) \wedge \Big(y_0{}^n - (y_0 - k_1)^n < k_1 n y_0{}^{n-1}\Big) \blacksquare y_0{}^n - t^n < k_1 n y_0{}^{n-1}$

(1.23.8.4) $(k_1 n y_0{}^{n-1} = y_0{}^n - x) \wedge (y_0{}^n - t^n < k_1 n y_0{}^{n-1}) \blacksquare y_0{}^n - t^n < y_0{}^n - x \blacksquare -t^n < -x \blacksquare t^n > x$

(1.23.8.5) $\big(t \in E \iff (t \in \mathbb{R} \wedge t > 0 \wedge t^n < x)\big) \wedge (t^n > x) \blacksquare t \notin E$

(1.23.9) $t \ge y_0 - k_1 \implies t \notin E \blacksquare t \in E \implies t < y_0 - k_1 \blacksquare \forall_{t\in E}(t \le y_0 - k_1) \blacksquare UpperBound[y_0 - k_1, E, \mathbb{R}, <]$

(1.23.10) $\big(LUB[y_0, E, \mathbb{R}, <] \wedge (y_0 - k_1 < y_0)\big) \blacksquare \neg UpperBound[y_0 - k_1, E, \mathbb{R}, <]$

(1.23.11) $(UpperBound[y_0 - k_1, E, \mathbb{R}, <]) \wedge (\neg UpperBound[y_0 - k_1, E, \mathbb{R}, <]) \blacksquare \bot$

(1.24) $y_0{}^n > x \implies \bot \blacksquare y_0{}^n \le x$

(1.25) $Order[\mathbb{R}, <] \blacksquare OrderTrichotomy[\mathbb{R}, <]$

(1.26) $(OrderTrichotomy[\mathbb{R}, <]) \wedge (y_0{}^n \ge x) \wedge (y_0{}^n \le x) \blacksquare y_0{}^n = x$

(1.27) $(y_0{}^n = x) \wedge (y_0 \in \mathbb{R}) \blacksquare \exists_{y\in\mathbb{R}}(y^n = x)$

(1.28) $y_1, y_2 := choice(\{y \in \mathbb{R} : y^n = x\})$

(1.29) $y_1 \ne y_2 \implies \dots$

(1.29.1) $(OrderTrichotomy[\mathbb{R}, <]) \wedge (y_1 \ne y_2) \blacksquare (y_1 < y_2) \veebar (y_2 < y_1) \; \dots$

(1.29.2) $\dots (x = y_1{}^n < y_2{}^n = x) \veebar (x = y_2{}^n < y_1{}^n = x) \blacksquare (x < x) \veebar (x > x) \blacksquare \bot \veebar \bot \blacksquare \bot$

(1.30) $y_1 \ne y_2 \implies \bot \blacksquare y_1 = y_2 \blacksquare \forall_{a,b\in\mathbb{R}}\big((a^n = x \wedge b^n = x) \implies a = b\big)$

(1.31) $\Big(\exists_{y\in\mathbb{R}}(y^n = x)\Big) \wedge \Big(\forall_{a,b\in\mathbb{R}}\big((a^n = x \wedge b^n = x) \implies a = b\big)\Big) \blacksquare \exists!_{y\in\mathbb{R}}(y^n = x)$

(2) $(0 < x \in \mathbb{R} \wedge 0 < n \in \mathbb{Z}) \implies \exists!_{y\in\mathbb{R}}(y^n = x) \blacksquare \forall_{0<x\in\mathbb{R}}\forall_{0<n\in\mathbb{Z}}\exists!_{0<y\in\mathbb{R}}(y_0{}^n = x)$

$RootExistenceInRCorollary := \forall_{0<a\in\mathbb{R}}\forall_{0<b\in\mathbb{R}}\forall_{0<n\in\mathbb{Z}}\Big((ab)^{1/n} = a^{1/n}b^{1/n}\Big)$ —

$$ExtendedRealSystem[\bar{\mathbb{R}}, +, *, <] := \left(\begin{array}{l} \bar{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\} \quad \wedge \quad -\infty < x < \infty \quad \wedge \\ x + \infty = +\infty \ \wedge \ x - \infty = -\infty \ \wedge \ \frac{x}{+\infty} = \frac{x}{-\infty} = 0 \ \wedge \\ (x > 0) \implies \big(x * (+\infty) = +\infty \wedge x * (-\infty) = -\infty\big) \wedge \\ (x < 0) \implies \big(x * (+\infty) = -\infty \wedge x * (-\infty) = +\infty\big) \end{array}\right)$$

$\mathbb{C} := \{\langle a, b\rangle \in \mathbb{R} \times \mathbb{R}\}$
$+_{\mathbb{C}}[\langle a, b\rangle, \langle c, d\rangle] := \langle a +_{\mathbb{R}} c, b +_{\mathbb{R}} d\rangle$
$*_{\mathbb{C}}[\langle a, b\rangle, \langle c, d\rangle] := \langle a *_{\mathbb{R}} c - b *_{\mathbb{R}} d, a *_{\mathbb{R}} d + b *_{\mathbb{R}} c\rangle$

$FieldC := Field[\mathbb{C}, +_{\mathbb{C}}, *_{\mathbb{C}}]$ —
$RSubfieldC := Subfield[\mathbb{R}, \mathbb{C}, +, *]$ —

$i := \langle 0, 1\rangle \in \mathbb{C}$

$iProperty := i^2 = -1$ —
$CProperty := (a, b \in \mathbb{R}) \implies (\langle a, b\rangle = a + bi)$ —

$Conjugate[\overline{a+bi}] := a - bi$

$ConjugateProperties := (w, z \in \mathbb{C}) \implies \dots$ —

(1)	$\overline{z+w} = \overline{z} + \overline{w}$
(2)	$\overline{z*w} = \overline{z} * \overline{w}$
(3)	$Re(z) = (1/2)(z+\overline{z}) \wedge Im(z) = (1/2)(z-\overline{z})$
(4)	$0 \leq z * \overline{z} \in \mathbb{R}$

$AbsoluteValueC[|z|] = (z * \overline{z})^{1/2}$
$AbsoluteValueProperties := (z, w \in \mathbb{C}) \implies \dots$ —

(1)	123123

TODO: - MORE EXPLICIT MODUS PONENS ON OrderTrichotomyR ??? - name all properties - hyperlink all definitions ???

Chapter 2

Abstract Algebra

2.1 Functions

$Rel[r, X] := (X \neq \emptyset) \wedge (r \subseteq X)$
$Func[f, X, Y] := (Rel[f, X \times Y]) \wedge \left(\forall_{x \in X} \exists!_{y \in Y} (\langle x, y \rangle \in f)\right)$
$Comp[g \circ f, f, g, X, Y, Z] := (Func[f, X, Y]) \wedge (Func[g, Y, Z]) \wedge (Func[g \circ f, X, Z]) \wedge \left(g \circ f = \{\langle x, g\big(f(x)\big)\rangle \in X \times Z | x \in X\}\right)$

$CompAssoc := h \circ (g \circ f) = (h \circ g) \circ f$

(1) TODO

$Domain[dom(f), f, X, Y] := (Func[f, X, Y]) \wedge \big(dom(f) = X\big)$
$Codomain[cod(f), f, X, Y] := (Func[f, X, Y]) \wedge \big(cod(f) = Y\big)$
$Image[im(A), A, f, X, Y] := (Func[f, X, Y]) \wedge (A \subseteq X) \wedge \big(im(A) = \{f(a) \in Y | a \in A\}\big)$
$Preimage[pim(B), B, f, X, Y] := (Func[f, X, Y]) \wedge (B \subseteq Y) \wedge \big(pim(B) = \{a \in X | f(a) \in B\}\big)$
$Range[rng(f), f, X, Y] := (Func[f, X, Y]) \wedge \big(Image[rng(f), dom(f), f, X, Y]\big)$

$Inj[f, X, Y] := (Func[f, X, Y]) \wedge \left(\forall_{x_1, x_2 \in X} \Big(\big(f(x_1) = f(x_2)\big) \implies (x_1 = x_2)\Big)\right)$
$Surj[f, X, Y] := (Func[f, X, Y]) \wedge \left(\forall_{y \in Y} \exists_{x \in X} \big(y = f(x)\big)\right)$
$Bij[f, X, Y] := (Inj[f, X, Y]) \wedge (Surj[f, X, Y])$
$Inv[f^{-1}, f, X, Y] := (Func[f, X, Y]) \wedge (Func[f^{-1}, Y, X]) \wedge (f \circ f^{-1} = I_Y) \wedge (f^{-1} \circ f = I_X)$

$SurjEquiv := (Surj[f, X, Y]) \iff \big(rng(f) = cod(f)\big)$

(1) TODO

$BijEquiv := (Bij[f, X, Y]) \iff \left(\exists_{f_{-1}} (Inv[f^{-1}, f, X, Y])\right)$

(1) TODO

$InjComp := \big((Inj[f]) \wedge (Inj[g])\big) \implies (Inj[g \circ f])$

(1) TODO

$SurjComp := \big((Surj[f]) \wedge (Surj[g])\big) \implies (Surj[g \circ f])$

(1) TODO

2.2 Divisibility, Equivalence Relations, Paritions

$DivisionAlgorithm := \forall_{b \in \mathbb{Z}} \forall_{a \in \mathbb{Z}^+} \exists!_{q, r \in \mathbb{Z}} \big((b = aq + r) \wedge (0 \leq r < a)\big)$

(1) TODO

$Divides[a,b] := (a, b \in \mathbb{Z}) \wedge \left(\exists_{c \in \mathbb{Z}}(b = ac)\right)$
$ComDiv[a,b,c] := (Divides[a,b]) \wedge (Divides[a,c])$
$GCD[a,b,c] := (ComDiv[a,b,c]) \wedge \left(\forall_{d \in \mathbb{Z}}\left(\left((Divides[d,b]) \wedge (Divides[d,c])\right) \implies (Divides[d,a])\right)\right)$
$RelPrime[a,b] := GCD[1,a,b]$
$CongRel[a,b,n] := Divides[n, a-b]$

$Partition[\mathcal{P}, S] := \left(\forall_{P \in \mathcal{P}}(P \neq \emptyset)\right) \wedge \left(S = \cup_{P \in \mathcal{P}}(P)\right) \wedge \left(\forall_{P_1, P_2 \in \mathcal{P}}\left((P_1 \neq P_2) \implies (P_1 \cap P_2 = \emptyset)\right)\right)$
$EqRel[\sim, S] := (Rel[\sim, S]) \wedge \left(\forall_{a \in S}(a \sim a)\right) \wedge \left(\forall_{a,b \in S}\left((a \sim b) \implies (b \sim a)\right)\right) \wedge \left(\forall_{a,b,c \in S}\left(\left((a \sim b) \wedge (b \sim c)\right) \implies (a \sim c)\right)\right)$
$EqClass[[s], s, \sim, S] := (Rel[\sim, S]) \wedge (s \in S) \wedge ([s] = \{x \in S | x \sim s\})$

$PartitionInducesEqRel := (Partition[\mathcal{P}, S]) \implies \left(\exists_{\sim}(EqRel[\sim, S])\right)$

(1) TODO : $\sim = \{\langle a, b\rangle \in S \times S | (P \in \mathcal{P}) \wedge (a, b \in P)\}$

$EqRelInducesPartition := (EqRel[\sim, S]) \implies \left(\exists_{\mathcal{P}}(Partition[\mathcal{P}, S])\right)$

(1) TODO : $Partition[EqClass_1, EqClass_2, \ldots]$

$EqRelCong := \forall_{n \in \mathbb{Z}^+}(EqRel[CongRel, \mathbb{Z}])$

(1) TODO

2.3 Groups

$$Group[G,*] := \begin{pmatrix} (Function[*, G, G]) \quad \wedge \\ \left(\forall_{a,b,c \in G}\left((a*b)*c = a*(b*c)\right)\right) \wedge \\ \left(\exists_{e \in G}\forall_{a \in G}(a*e = a = e*a)\right) \quad \wedge \\ \left(\forall_{a \in G}\exists_{a^{-1} \in G}(a*a^{-1} = e = a^{-1}*a)\right) \end{pmatrix}$$

$AbelianGroup[G,*] := (Group[G,*]) \wedge \left(\forall_{a,b \in G}(a*b = b*a)\right)$

$CancelLaws := \forall_G\left((Group[G,*]) \implies \left(\forall_{a,b,c \in G}\left(\left((a*b = a*c) \implies (b=c)\right) \wedge \left((a*c = b*c) \implies (a=b)\right)\right)\right)\right)$

(1) $(a*b = a*c) \implies \ldots$

(1.1) $a \in G \;\blacksquare\; \exists_{a^{-1} \in G}(a*a^{-1} = e = a^{-1}*a)$

(1.2) $Function[*, G, G] \;\blacksquare\; a^{-1}*a*b = a^{-1}*a*c$

(1.3) $\left(\forall_{a,b,c \in G}\left((a*b)*c = a*(b*c)\right)\right) \wedge \left(\forall_{a \in G}\exists_{a^{-1} \in G}(a*a^{-1} = e = a^{-1}*a)\right) \;\blacksquare\; b = c$

(2) $(a*b = a*c) \implies (b=c)$

(3) $(a*c = b*c) \implies \ldots$

(3.1) TODO

(4) $(a*c = b*c) \implies (a=b)$

(5) $\left((a*b = a*c) \implies (b=c)\right) \wedge \left((a*c = b*c) \implies (a=b)\right)$

$IdUniq := \forall_G\left((Group[G,*]) \implies \left(\forall_{e_1, e_2 \in G}\forall_{a \in G}\left(\left((a*e_1 = a = e_1*a) \wedge (a*e_2 = a = e_2*a)\right) \implies (e_1 = e_2)\right)\right)\right)$

(1) $(CancelLaws) \wedge \left(\forall_{a \in G}\exists_{a^{-1} \in G}(a*a^{-1} = e = a^{-1}*a)\right) \;\blacksquare\; a*e_1 = a = a*e_2 \;\blacksquare\; e_1 = e_2$

$InvUniq := \forall_G\left((Group[G,*]) \implies \left(\forall_{a \in G}\forall_{a_1^{-1}, a_2^{-1} \in G}\left(\left((a*a_1^{-1} = e = a_1^{-1}*a) \wedge (a*a_2^{-1} = e = a_2^{-1}*a)\right) \implies (a_1^{-1} = a_2^{-1})\right)\right)\right)$

(1) $(CancelLaws) \wedge \left(\forall_{a \in G} \exists_{a^{-1} \in G} (a * a^{-1} = e = a^{-1} * a)\right) \blacksquare\ a * a_1^{-1} = e = a * a_2^{-1} \blacksquare\ a_1^{-1} = a_2^{-1}$

$InvProd := \forall_G \forall_{a,b \in G} \left((a * b)^{-1} = b^{-1} * a^{-1}\right)$

(1) $(a * b) * (a * b)^{-1} = e$

(2) $(a * b) * (b^{-1} * a^{-1}) = \left(a * (b * b^{-1}) * a^{-1}\right) = e$

(3) $InvUniq \blacksquare\ (a * b)^{-1} = b^{-1} * a^{-1}$

$OrderEl[o(G), G, *] := (Group[G, *]) \wedge \left(o(G) = |G|\right)$
$gWitness[n, g, G, *] := (Group[G, *]) \wedge (n \in \mathbb{Z}^+) \wedge (g^n = e) \wedge \left(\forall_{m \in \mathbb{Z}^+} (m < n) \implies (g^m \neq e)\right)$
$OrderEl[o(g), g, G, *] := (Group[G, *]) \wedge \Big(\left(\exists_n (gWitness[n, g, G, *])\right) \implies \left(o(g) = n\right)\Big) \wedge \Big(\left(\neg \exists_n (gWitness[n, g, G, *])\right) \implies \left(o(g) = \infty\right)\Big)$

2.4 Subgroups

$Subgroup[H, G, *] := (Group[G, *]) \wedge (H \subseteq G) \wedge (Group[H, *])$
$TrivSubgroup[H, G, *] := (H = \{e\}) \vee (H = G)$
$PropSubgroup[H, G, *] := (Subgroup[H, G, *]) \wedge (\neg TrivSubgroup[H, G, *])$

$$SubgroupEquiv := \forall_{H,G} \left(\begin{array}{c} (Subgroup[H, G, *]) \qquad \iff \\ \left((Group[G, *]) \wedge (\emptyset \neq H \subseteq G) \wedge (Function[*, H, H]) \wedge \left(\forall_{a \in H} \exists_{a^{-1} \in H} (a * a^{-1} = e = a^{-1} * a)\right)\right) \end{array} \right)$$

(1) $(Subgroup[H, G, *]) \implies \left((\emptyset \neq H \subseteq G) \wedge (Function[*, H, H]) \wedge \left(\forall_{a \in H} \exists_{a^{-1} \in H} (a * a^{-1} = e = a^{-1} * a)\right)\right)$

(2) $\left((\emptyset \neq H \subseteq G) \wedge (Function[*, H, H]) \wedge \left(\forall_{a \in H} \exists_{a^{-1} \in H} (a * a^{-1} = e = a^{-1} * a)\right)\right) \implies \ldots$

(2.1) $Group[G, *] \blacksquare\ (a, b, c \in H) \implies (a, b, c \in G) \implies \left((a * b) * c = a * (b * c)\right) \blacksquare\ \forall_{a,b,c \in H} \left((a * b) * c = a * (b * c)\right)$

(2.2) $\emptyset \neq H \blacksquare\ \exists_h (h \in H)$

(2.3) $h \in H \blacksquare\ \exists_{h^{-1} \in H} (h * h^{-1} = e = h^{-1} * h)$

(2.4) $Function[*, H, H] \blacksquare\ e = h * h^{-1} \in H \blacksquare\ e \in H \blacksquare\ \exists_{e \in H} \forall_{a \in H} (a * e = a = e * a)$

(2.5) $(Function[*, H, H]) \wedge \left(\forall_{a,b,c \in H} \left((a * b) * c = a * (b * c)\right)\right) \wedge \left(\exists_{e \in H} \forall_{a \in H} (a * e = a = e * a) \wedge (\forall_{a \in H} \exists_{a^{-1} \in H} (a * a^{-1} = e = a^{-1} * a)\right)$

(2.6) $Group[H, *]$

(2.7) $(Group[G, *]) \wedge (H \subseteq G) \wedge (Group[H, *]) \blacksquare\ Subgroup[H, G, *]$

(3) $\left((\emptyset \neq H \subseteq G) \wedge (Function[*, H, H]) \wedge \left(\forall_{a \in H} \exists_{a^{-1} \in H} (a * a^{-1} = e = a^{-1} * a)\right)\right) \implies (Subgroup[H, G, *])$

(4) $(Subgroup[H, G, *]) \iff \left((Group[G, *]) \wedge (\emptyset \neq H \subseteq G) \wedge (Function[*, H, H]) \wedge \left(\forall_{a \in H} \exists_{a^{-1} \in H} (a * a^{-1} = e = a^{-1} * a)\right)\right)$

$$SubgroupEquivOST := \forall_{H,G} \left((Subgroup[H, G, *]) \iff \left((Group[G, *]) \wedge (\emptyset \neq H \subseteq G) \wedge \left(\forall_{a,b \in H} (a * b^{-1} \in H)\right)\right)\right)$$

(1) TODO

$SubgroupIntersection := \forall_{H_1, H_2, G} \Big(\left((Subgroup[H_1, G, *]) \wedge (Subgroup[H_2, G, *])\right) \implies (Subgroup[H_1 \cap H_2, G, *])\Big)$

(1) $Group[G, *]$

(2) $(e \in H_1) \wedge (e \in H_2) \blacksquare\ e \in H_1 \cap H_2 \blacksquare\ \emptyset \neq H_1 \cap H_2$

(3) $(H_1 \subseteq G) \wedge (H_2 \subseteq G) \blacksquare\ H_1 \cap H_2 \subseteq G$

(4) $\emptyset \neq H_1 \cap H_2 \subseteq G$

(5) $(a, b \in H_1 \cap H_2) \implies \ldots$

(5.1) $a, b \in H_1 \blacksquare\ a * b \in H_1$

(5.2) $a, b \in H_2 \blacksquare\ a * b \in H_2$

(5.3) $a * b \in H_1 \cap H_2$

(6) $(a, b \in H_1 \cap H_2) \implies (a * b \in H_1 \cap H_2) \blacksquare Function[*, H_1 \cap H_2, H_1 \cap H_2]$

(7) $(a \in H_1 \cap H_2) \implies \ldots$

(7.1) $(a^{-1} \in H_1) \wedge (a^{-1} \in H_2) \blacksquare a^{-1} \in H_1 \cap H_2$

(8) $(a \in H_1 \cap H_2) \implies (a^{-1} \in H_1 \cap H_2) \blacksquare \forall_{a \in H_1 \cap H_2} \exists_{a^{-1} \in H_1 \cap H_2} (a * a^{-1} = e = a^{-1} * a)$

(9) $(SubgroupEquiv) \wedge (Group[G, *]) \wedge (\emptyset \neq H_1 \cap H_2 \subseteq G) \wedge (Function[*, H_1 \cap H_2, H_1 \cap H_2]) \wedge \ \ldots$

(10) $\ldots \left(\forall_{a \in H_1 \cap H_2} \exists_{a^{-1} \in H_1 \cap H_2} (a * a^{-1} = e = a^{-1} * a)\right) \blacksquare Subgroup[H_1 \cap H_2, G, *]$

$Centralizer[C(g), g, G, *] := (Group[G, *]) \wedge (g \in G) \wedge \big(C(g) = \{h \in G | g * h = h * g\}\big)$

$SubgroupCentralizer := \forall_{g,G}\Big(\big(Centralizer[C(g), g, G, *]\big) \implies \big(Subgroup[C(g), G, *]\big)\Big)$

(1) $e * g = g * e \blacksquare e \in C(g) \blacksquare C(g) \neq \emptyset$

(2) $C(g) \subseteq G \blacksquare \emptyset \neq C(g) \subseteq G$

(3) $\big(a, b \in C(g)\big) \implies \ldots$

(3.1) $(a * g = g * a) \wedge (b * g = g * b)$

(3.2) $(a * b) * g = a * (b * g) = a * (g * b) = (a * g) * b = (g * a) * b = g * (a * b) \blacksquare a * b \in C(g)$

(4) $\big(a, b \in C(g)\big) \implies \big(a * b \in C(g)\big) \blacksquare \forall_{a,b \in C(g)}\big(a * b \in C(g)\big)$

(5) $\big(a \in C(g)\big) \implies \ldots$

(5.1) $a * g = g * a$

(5.2) $a^{-1} * (a * g) * a^{-1} = a^{-1} * (g * a) * a^{-1} \blacksquare g * a^{-1} = a^{-1} * g \blacksquare a^{-1} \in C(g)$

(6) $\big(a \in C(g)\big) \implies \Big(a^{-1} \in C(g)\Big) \blacksquare \forall_{a \in C(g)}\Big(a^{-1} \in C(g)\Big)$

(7) $(SubgroupEquiv) \wedge \big(\emptyset \neq C(g) \subseteq G\big) \wedge \Big(\forall_{a,b \in C(g)}\big(a * b \in C(g)\big)\Big) \wedge \Bigg(\forall_{a \in C(g)}\Big(a^{-1} \in C(g)\Big)\Bigg) \blacksquare Subgroup[C(g), G, *]$

$Center[Z(G), G, *] := (Group[G, *]) \wedge \Big(Z(G) = \cap_{g \in G}\big(C(g)\big)\Big)$

$SubgroupCenter := \forall_G\Big(\big(Center[Z(G), G, *]\big) \implies \big(Subgroup[Z(G), G, *]\big)\Big)$

(1) $(SubgroupCentralizer) \wedge (SubgroupIntersection) \blacksquare Subgroup[Z(G), G, *]$

2.5 Special Groups

2.5.1 Cyclic Group

$CyclicSubgroup[< g >, g, G, *] := (Group[G, *]) \wedge (g \in G) \wedge (< g >= \{g^n | n \in \mathbb{Z}\})$
$Generator[g, G, *] := CyclicSubgroup[G, g, G, *]$
$CyclicGroup[G, *] := \exists_{g \in G}(Generator[g, G, *])$

$SubgroupOfCyclicGroupIsCyclic := \forall_{G,H}\Big(\big((CyclicGroup[G, *]) \wedge (Subgroup[H, G, *])\big) \implies (CyclicGroup[H, *])\Big)$

(1) $\exists_{g \in G}(Generator[g, G, *])$

(2) $H \subseteq G \blacksquare \exists_{m \in \mathbb{Z}^+}\Bigg((g^m \in H) \wedge \Big(\forall_{k \in \mathbb{Z}^+}\big((k < m) \implies (g^k \notin H)\big)\Big)\Bigg)$

(3) $(b \in H) \implies \ldots$

(3.1) $H \subseteq G \blacksquare \exists_{n \in \mathbb{Z}^+}(b = g^n)$

(3.2) $(DivisionAlgorithm) \wedge (n \in \mathbb{Z}) \wedge (m \in \mathbb{Z}^+) \blacksquare \exists!_{q,r \in \mathbb{Z}}\big((n = mq + r) \wedge (0 \leq r < m)\big)$

(3.3) $g^n = g^{mq+r} = g^{mq} * g^r \blacksquare g^r = (g^{mq})^{-1} * g^n$

(3.4) $g^n, g^m \in H \blacksquare g^n, (g^{mq})^{-1} \in H \blacksquare g^r = (g^{mq})^{-1} * g^n \in H \blacksquare g^r \in H$

(3.5) $(g^r \in H) \wedge (0 \leq r < m) \wedge \Big(\forall_{k \in \mathbb{Z}^+}\big((k < m) \implies (g^k \notin H)\big)\Big) \blacksquare r = 0$

(3.6) $(r = 0) \wedge (g^n = g^{mq+r}) \wedge (b = g^n) \blacksquare b = g^n = g^{mq} \blacksquare b \in < g^m >$

(4) $(b \in H) \implies (b \in < g^m >) \blacksquare H \subseteq < g^m >$
(5) $(b \in < g^m >) \implies \dots$
(5.1) $\exists_{k \in \mathbb{Z}}(b = g^{mk})$
(5.2) $g^m \in H \blacksquare b = g^{mk} \in H \blacksquare b \in H$
(6) $(b \in < g^m >) \implies (b \in H) \blacksquare < g^m > \subseteq H$
(7) $(H \subseteq < g^m >) \wedge (< g^m > \subseteq H) \blacksquare H = < g^m > \blacksquare Generator[g^m, H, *] \blacksquare \exists_{h \in G}(Generator[h, G, *]) \blacksquare CyclicGroup[H, *]$

$$ExpModOrder := \forall_{G,g,n,s,t}\Big((Group[G,*]) \wedge (g \in G) \wedge (OrderEl[n,g,G,*]) \implies \big((g^s = g^t) \iff \big(s \equiv t(mod\ n)\big)\big)\Big)$$

(1) TODO

2.5.2 Symmetric and Alternating Groups

$SymmetricGroup[S_n, n] := S_n = \{\text{permutation of a set with n elements}\}$
$SymmetricGroupOrder := o(S_n) = n!$
$SymmetricGroupAsDisjoinsCycles := \forall_{\sigma \in S_n}\exists_{\Sigma \subseteq S_n}\Big((DisjointCycles[\Sigma]) \wedge \big(\sigma = \prod(\sigma_i)\big)\Big)$
$SymmetricGroupAsTranspositions := \forall_{\sigma \in S_n}\exists_{\Sigma \subseteq S_n}\Big((Transpositions[\Sigma]) \wedge \big(\sigma = \prod(\sigma_i)\big)\Big)$

$\upsilon Function[\upsilon(\sigma), \sigma, S_n] := \upsilon(\sigma) = n - |DisjointFullCycles[\Sigma]|$
$signFunction[sign(\sigma), \sigma, S_n] := sign(\sigma) = (-1)^{\upsilon(\sigma)}$
$EvenPermutation[\sigma, S_n] := sign(\sigma) = 1$
$OddPermutation[\sigma, S_n] := sign(\sigma) = -1$

$TranspositionSigns := sign(\tau\sigma) = -sign(\sigma)$
$TranspositionSignsCorollary := sign\big(\prod_{i=1}^{r}(\tau_i)\big) = (-1)^r$
$SignProp := sign(\sigma\pi) = sign(\sigma)sign(\pi)$

$AlternatingGroup[A_n, n] := A_n = \{\sigma \in S_n | EvenPermutation[\sigma, S_n]\}$
$AlternatingGroupOrder := o(A_n) = n!/2$

2.5.3 Dihedral Group

$$DihedralGroup[D_n,*] := \big(D_n = \{a^r * b^s | (r \in \mathbb{N}_{0,n-1}) \wedge (s \in \mathbb{N}_{0,1})\}\big) \wedge \left(\begin{array}{l} \big(a^p a^q = a^{(p+q)\%n}\big) \wedge \\ \big(a^p b a^q = a^{(p-q)\%n} b\big) \wedge \\ \big(a^p b a^q b = a^{(p-q)\%n}\big) \end{array}\right)$$

$DihedralGroupOrder := o(D_n) = 2n$

2.6 Lagrange's Theorem

$LeftCoset[gH, g, H, G, *] := (Subgroup[H, G, *]) \wedge (g \in G) \wedge (gH = \{g * h | h \in H\})$
$RightCoset[Hg, g, H, G, *] := (Subgroup[H, G, *]) \wedge (g \in G) \wedge (Hg = \{h * g | h \in H\})$

$CosetCardinality := (RightCoset[Hg, g, H, G, *]) \implies (|H| = |Hg|)$

(1) $CancellationLaws \blacksquare (h_1 g = h_2 g) \implies (h_1 = h_2) \blacksquare |H| = |Hg|$

$$CosetInduceEqRel := \forall_{G,H}\Big(\big((Subgroup[H,G,*]) \wedge (\sim = \{\langle a,b \rangle | a * b^{-1} \in H\})\big) \implies \big((EqRel[\sim, G]) \wedge (EqClass[Ha, a, \sim, G])\big)\Big)$$

(1) $(a, b, c \in G) \implies \dots$
(1.1) $(Subgroup[H, G, *]) \implies (e \in H) \implies (a * a^{-1} \in H) \implies (a \sim a)$
(1.2) $(a \sim b) \implies (a * b^{-1} \in H) \implies \big(b * a^{-1} = (a * b^{-1})^{-1} \in H\big) \implies (b \sim a)$

(1.3) $\left((a \sim b) \wedge (b \sim c)\right) \implies (a * b^{-1}, b * c^{-1} \in H) \implies \left(a * c^{-1} = (a * b^{-1}) * (b * c^{-1}) \in H\right) \;\blacksquare\; a \sim c$

(2) $EqRel[\sim, G]$

(3) $(a, x \in G) \implies \ldots$

(3.1) $(x \sim a) \iff (x * a^{-1} \in H) \iff \left(\exists_{h \in H}(x * a^{-1} = h)\right) \iff \left(\exists_{h \in H}(x = h * a)\right) \iff (x \in Ha)$

(4) $[a] = \{x \in G | x \sim a\} = Ha$

$LagrangeTheorem := \forall_{G,H}\left(\left((Order[n, G, *]) \wedge (Order[m, H, *]) \wedge (n, m \in \mathbb{N}) \wedge (Subgroup[H, G, *])\right) \implies (Divides[m, n])\right)$

(1) $(CosetInduceEqRel) \wedge (EqRelInducesPartition) \wedge (CosetCardinality) \;\blacksquare\; \exists_{k \in \mathbb{N}}(n = mk) \;\blacksquare\; Divides[m, n]$

$IndexSubgroup[|G : H|, H, G, *] := (Subgroup[H, G, *]) \wedge (|G : H| =$ Number of distinct right cosets of H, i.e., k in LagrangeTheorem$)$

$OrderOrderElProp := \forall_{g,G}\left(\left((Order[n, G, *]) \wedge (OrderEl[m, g, G, *])\right) \implies \left((Divides[m, n]) \wedge (g^n = e)\right)\right)$

(1) $CyclicSubgroup[< g >, g, G, *] \;\blacksquare\; Order[< g >] = m$

(2) $(LagrangeTheorem) \wedge (CyclicSubgroup) \;\blacksquare\; Divides[Order[< g >], Order[G]] \;\blacksquare\; Divides[m, n]$

(3) $g^n = g^{mk} = e^k = e$

Any prime ordered cyclic group has no proper non-trivial subgroups and any non-identity element is a generator.

(1) $LagrangeTheorem$ $\blacksquare$ Subgroups must have the order 1 or p $\blacksquare$ Subgroups are trivial

(2) CyclicSubgroup of a non-identity element is G $\blacksquare$ Non-identity elements generates G

$\left((Subgroup[H, G, *]) \wedge \left(Subgroup[K, G, *] \wedge \left(RelPrime(o(H), o(K))\right)\right)\right) \implies (H \cap K = \{e\})$

(1) TODO

2.7 Homomorphisms

$Homomorphism[\phi, G, *, H, \diamond] := (Function[\phi, G, H]) \wedge \left(\forall_{a,b \in G}\left(\phi(a * b) = \phi(a) \diamond \phi(b)\right)\right)$
$Monomorphism[\phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \wedge (Inj[\phi, G, H])$
$Epimorphism[\phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \wedge (Surj[\phi, G, H])$
$Isomorphism[\phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \wedge (Bij[\phi, G, H])$
$Isomorphic[G, *, H, \diamond] := \exists_{\phi}(Isomorphism[\phi, G, *, H, \diamond])$ ** Notation: $G \cong H$ **
$Automorphism[\phi, G, *] := Isomorphism[\phi, G, *, G, *]$

$IdMapsId := (Homomorphism[\phi, G, *, H, \diamond]) \implies \left(\phi(e_G) = e_H\right)$

(1) $\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \diamond \phi(e_G)$

(2) $e_H = \phi(e_G)^{-1} \diamond \phi(e_G) = \phi(e_G)^{-1} \diamond \phi(e_G) \diamond \phi(e_G) = \phi(e_G)$

$InvMapsInv := (Homomorphism[\phi, G, *, H, \diamond]) \implies \left(\phi(g^{-1}) = \phi(g)^{-1}\right)$

(1) $IdMapsId \;\blacksquare\; e_H = \phi(e_G) = \phi(g * g^{-1}) = \phi(g) \diamond \phi(g^{-1}) \;\blacksquare\; e_H = \phi(g) \diamond \phi(g^{-1}) \;\blacksquare\; \phi(g^{-1}) = \phi(g)^{-1}$

$ExpMapsExp := (Homomorphism[\phi, G, *, H, \diamond]) \implies \left(\phi(g^n) = \phi(g)^n\right)$

(1) $\phi(g^n) = \phi(g * \ldots * g) = \phi(g) \diamond \ldots \phi(g) = \phi(g)^n$

$MapDivProp := \left((Homomorphism[\phi, G, *, H, \diamond]) \wedge (Order[n, G, *])\right) \implies \left(\forall_{g \in G}\left(\left(OrderEl[m, \phi(g), H, \diamond]\right) \implies (Divides[m, n])\right)\right)$

(1) $OrderOrderElProp \;\blacksquare\; g^n = e_G$

(2) $(IdMapsId) \wedge (ExpMapsExp) \;\blacksquare\; e_G = \phi(g^n) = \phi(g)^n = e_H$

(3) $OrderEl[m, \phi(g), H, \diamond] \;\blacksquare\; \phi(g)^m = e_H \;\blacksquare\; \phi(g)^m = e_H = {e_H}^k = \phi(g)^n$

$HomoCompInduceHomo := \big((Homomorphism[\phi, G, *, H, \diamond]) \land (Homomorphism[\theta, H, \diamond, K, \square])\big) \implies (Homomorphism[\theta\circ\phi, G, *, K, \square])$

(1) TODO

$IsoInvInduceIso := (Isomorphism[\phi, G, *, H, \diamond]) \implies (Isomorphism[\phi^{-1}, H, \diamond, G, *])$

(1) TODO

$KCycleGroupIsomorphic := \left(\begin{array}{l} \big((CyclicGroup[G, *]) \land (CyclicGroup[H, \diamond]) \land (Order[n, G, *]) \land (Order[n, H, \diamond])\big) \implies \\ (Isomorphic[G, *, H, \diamond]) \end{array} \right)$

(1) TODO

2.8 Kernel and Image Homomorphisms

$Kernel[ker_\phi, \phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \land \Big(ker_\phi = \{g \in G | \phi(g) = e_H\}\Big)$

$Image[im_\phi, \phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \land \Big(im_\phi = \{\phi(g) \in H | g \in G\}\Big)$

$KernelSubgroupDomain := (Homomorphism[\phi, G, *, H, \diamond]) \implies (Subgroup[ker_\phi, G, *])$

(1) $IdMapsId$ ▌ $\phi(e_G) = e_H$ ▌ $e_G \in ker_\phi$ ▌ $ker_\phi \neq \emptyset$

(2) $ker_\phi \subseteq G$ ▌ $\emptyset \neq ker_\phi \subseteq G$

(3) $(a, b \in ker_\phi) \implies \ldots$

(3.1) $\big(\phi(a) = e_H\big) \land \big(\phi(b) = e_H\big)$ ▌ $e_H = e_H \diamond e_H = \phi(a) \diamond \phi(b) = \phi(a * b)$ ▌ $a * b \in ker_\phi$

(4) $(a, b \in ker_\phi) \implies (a * b \in ker_\phi)$ ▌ $\forall_{a,b\in ker_\phi}(a * b \in ker_\phi)$

(5) $(a \in ker_\phi) \implies \ldots$

(5.1) $\phi(a) = e_H$

(5.2) $InvMapsInv$ ▌ $\phi(a^{-1}) = {e_H}^{-1} = e_H$ ▌ $a^{-1} \in ker_\phi$

(6) $(a \in ker_\phi) \implies (a^{-1} \in ker_\phi)$ ▌ $\forall_{a\in ker_\phi}(a^{-1} \in ker_\phi)$

(7) $(SubgroupEquiv) \land (\emptyset \neq ker_\phi \subseteq G) \land \Big(\forall_{a,b\in ker_\phi}(a * b \in ker_\phi)\Big) \land \Big(\forall_{a\in ker_\phi}(a^{-1} \in ker_\phi)\Big)$ ▌ $Subgroup[ker_\phi, G, *]$

$ImageSubgroupCodomain := (Homomorphism[\phi, G, *, H, \diamond]) \implies (Subgroup[im_\phi, H, \diamond])$

(1) TODO

$ImageCyclicIsCyclic := \big((Homomorphism[\phi, G, *, H, \diamond]) \land (CyclicGroup[G, *])\big) \implies (CyclicGroup[im_\phi, \diamond])$

(1) TODO

$MonomorphismEquiv := (Monomorphism[\phi, G, *, H, \diamond]) \iff (ker_\phi = \{e_G\})$

(1) $(Monomorphism[\phi, G, *, H, \diamond]) \implies \ldots$

(1.1) $IdMapsId$ ▌ $\phi(e_G) = e_H$ ▌ $e_G \in ker_\phi$ ▌ $\{e_G\} \subseteq ker_\phi$

(1.2) $(g \in ker_\phi) \implies \ldots$

(1.2.1) $(g \in ker_\phi) \land (IdMapsId)$ ▌ $\phi(g) = e_H = \phi(e_G)$

(1.2.2) $(Injective[\phi, G, H]) \land \big(\phi(g) = \phi(e_G)\big)$ ▌ $g = e_G$ ▌ $g \in \{e_G\}$

(1.3) $(g \in ker_\phi) \implies (g \in \{e_G\})$ ▌ $ker_\phi \subseteq \{e_G\}$

(1.4) $(\{e_G\} \subseteq ker_\phi) \land (ker_\phi \subseteq \{e_G\})$ ▌ $ker_\phi = \{e_G\}$

(2) $(Monomorphism[\phi, G, *, H, \diamond]) \implies (ker_\phi = \{e_G\})$

(3) $(ker_\phi = \{e_G\}) \implies \ldots$

(3.1) $\Big((g_1, g_2 \in G) \land \big(\phi(g_1) = \phi(g_2)\big)\Big) \implies \ldots$

(3.1.1) $InvMapsInv$ ▌ $e_H = \phi(g_1) \diamond \phi(g_2)^{-1} = \phi(g_1) \diamond \phi({g_2}^{-1}) = \phi(g_1 * {g_2}^{-1})$ ▌ $e_H = \phi(g_1 * {g_2}^{-1})$ ▌ $g_1 * {g_2}^{-1} \in ker_\phi$

(3.1.2) $(ker_\phi = \{e_G\}) \wedge (g_1 * {g_2}^{-1} \in ker_\phi) \;\blacksquare\; g_1 * {g_2}^{-1} = e_G \;\blacksquare\; {g_1}^{-1} = {g_2}^{-1}$

(3.1.3) $InvUniq \;\blacksquare\; g_1 = g_2$

(3.2) $\Big((g_1, g_2 \in G) \wedge \big(\phi(g_1) = \phi(g_2)\big)\Big) \implies (g_1 = g_2) \;\blacksquare\; Injective[\phi, G, H] \;\blacksquare\; Monomorphism[\phi, G, *, H, \diamond]$

(4) $(ker_\phi = \{e_G\}) \implies (Monomorphism[\phi, G, *, H, \diamond])$

(5) $\Big((Monomorphism[\phi, G, *, H, \diamond]) \implies (ker_\phi = \{e_G\})\Big) \wedge \Big((ker_\phi = \{e_G\}) \implies (Monomorphism[\phi, G, *, H, \diamond])\Big)$

(6) $(Monomorphism[\phi, G, *, H, \diamond]) \iff (ker_\phi = \{e_G\})$

$MapsToSameEl := (ker_\phi)g = \{x \in G | \phi(x) = \phi(g)\}$

(1) $\Big(x \in (ker_\phi)g\Big) \implies \ldots$

(1.1) $\exists_{K_x \in ker_\phi}(x = K_x * g) \;\blacksquare\; \phi(x) = \phi(K_x * g) = \phi(K_x) \diamond \phi(g) = e_H \diamond \phi(g) = \phi(g) \;\blacksquare\; \phi(x) = \phi(g)$

(2) $\Big(x \in (ker_\phi)g\Big) \implies \big(\phi(x) = \phi(g)\big) \;\blacksquare\; (ker_\phi)g \subseteq \{x \in G | \phi(x) = \phi(g)\}$

(3) $\big(\phi(x) = \phi(g)\big) \implies \ldots$

(3.1) $e_H = \phi(x) \diamond \phi(g)^{-1} = \phi(x) \diamond \phi(g^{-1)} = \phi(x * g^{-1)} \;\blacksquare\; x * g^{-1} \in ker_\phi \;\blacksquare\; x \in (ker_\phi)g$

(4) $\big(\phi(x) = \phi(g)\big) \implies \Big(x \in (ker_\phi)g\Big)$

$MapsToSameElMultiplicity := \Big((|G| = n) \wedge (|ker_\phi| = m) \wedge (|im_\phi| = r)\Big) \implies (n = mr)$

(1) TODO

$ImageDividesGH := (|im_\phi| = r) \implies \Big(\big(Divides[r, o(G)]\big) \wedge \big(Divides[r, o(H)]\big)\Big)$

(1) $MapsToSameElMultiplicity \;\blacksquare\; Divides[r, o(G)]$

(2) $LagrangeTheorem \;\blacksquare\; Divides[r, o(H)]$

2.9 Conjugacy

$Conjugate[\sim^*, a, b, G, *] := (Group[G, *]) \wedge (a, b \in G) \wedge \Big(\exists_{c \in G}(b = c^{-1} * a * c)\Big)$

$ConjugateEqRel := EqRel[\sim^*, G]$

(1) $(a, b, c \in G) \implies \ldots$

(1.1) $a = e^{-1} * a * e \;\blacksquare\; a \sim^* a$

(1.2) $(a \sim^* b) \implies (b = x_b^{-1} * a * x_b) \implies (x_b * b * x_b^{-1} = a) \implies (b \sim^* a)$

(1.3) $\big((a \sim^* b) \wedge (b \sim^* c)\big) \implies \Big((b = x_b^{-1} * a * x_b) \wedge (c = x_c^{-1} * b * x_c)\Big) \implies \;\ldots$

(1.4) $\ldots\Big(c = x_c^{-1} * x_b^{-1} * a * x_b * x_c = (x_b * x_c)^{-1} * a * (x_b * x_c)\Big) \;\blacksquare\; a \sim^* c$

(2) $EqRel[\sim^*, G]$

$ConjugacyClass[C_g, g, G, *] := (Group[G, *]) \wedge (g \in G) \wedge (EqClass[C_g, g, \sim^*, G])$

$ConjugacyCenter := (g \in G) \implies \Big((C_g = \{g\}) \iff \big(g \in Z(G)\big)\Big)$

(1) $\big(g \in Z(g)\big) \iff \big(\forall_{x \in G}(x * g = g * x)\big) \iff \Big(\forall_{x \in G}(x * g * x^{-1} = g)\Big) \iff \Big(\forall_{f \in G}\big((f \sim^* g) \iff (f = g)\big)\Big) \iff (C_g = \{g\})$

**Note: why is this both sound and awkward at the same time

$ConjugacyAbelian := \Big(\forall_{g \in G}(C_g = \{g\})\Big) \iff (AbelianGroup[G])$

(1) $ConjugacyCenter \;\blacksquare\; \Big(\forall_{g \in G}(C_g = \{g\})\Big) \iff \Big(\forall_{g \in G}\big(g \in Z(g)\big)\Big) \iff (AbelianGroup[G])$

$ConjugateOrder := (h \sim^{*} g) \implies \big(o(h) = o(g)\big)$

(1) $\exists_{c \in G}(g = c^{-1}hc)$ ▮ $e = g^{o(g)} = (c^{-1}hc)^{o(g)} = c^{-1}h^{o(g)}c$ ▮ $e = c^{-1}h^{o(g)}c$ ▮ $h^{o(g)} = e$ ▮ $o(h) = o(g)$

(2) TODO: contradiction if $h^m = e$ for some $m < o(g)$

Chapter 3

Linear Algebra

3.1 Matrix Operations and Special Matrices

$Matrix[A, m, n] := [a_{i,j}]_{m \times n}$:= m rows, n columns of real numbers
$\mathcal{M}_{m,n} := \{A : Matrix[A, m, n]\}$
$O_{m,n} := (Matrix[O, m, n]) \wedge (a_{i,j} = 0)$
$Square[A, n] := Matrix[A, n, n]$
$UpperTriangular[A] := (Square[A]) \wedge (i > j \implies a_{i,j} = 0)$
$LowerTriangular[A] := (Square[A]) \wedge (i < j \implies a_{i,j} = 0)$
$Diagonal[A, n] := (Square[A, n]) \wedge (i \neq j \implies a_{i,j} = 0)$
$Scalar[A, n, k] := (Diagonal[A, n]) \wedge (a_{i,i} = k)$
$I_n := Scalar[I, n, 1]$

$+(A, B) := \big((Matrix[A, m, n]) \wedge (Matrix[B, m, n])\big) \implies (A + B = [a_{i,j} + b_{i,j}]_{m \times n})$
$*\,(r, A) := \big((r \in \mathbb{R}) \wedge (Matrix[A, m, n])\big) \implies (r * A = [ra_{i,j}]_{m \times n})$
$*\,(A, B) := \big((Matrix[A, m, p]) \wedge (Matrix[B, p, n])\big) \implies \left(A * B = \left[\sum_{k=1}^{p}(a_{i,k} b_{k,j})\right]_{m \times n}\right)$
${}^T[A] := (Matrix[A, m, n]) \implies (A^T = [a_{j,i}]_{n \times m})$

$AddCom := \forall_{A,B \in \mathcal{M}}(A + B = B + A)$

(1) $A + B = [a_{i,j} + b_{i,j}] = [b_{i,j} + a_{i,j}] = B + A$

$AddAssoc := \forall_{A,B,C \in \mathcal{M}}\big((A + B) + C = A + (B + C)\big)$

(1) $(A + B) + C = [(a_{i,j} + b_{i,j}) + c_{i,j}] = [a_{i,j} + (b_{i,j} + c_{i,j})] = A + (B + C)$

$AddId := \forall_{A \in \mathcal{M}} \exists!_{O \in \mathcal{M}}(A + O = A = O + A)$

(1) $A + O = [a_{i,j} + 0] = A = [0 + a_{i,j}] = O + A$

(2) $A + O_1 = A = A + O_2 \;\blacksquare\; O_1 = O_2$

$AddInv := \forall_{A \in \mathcal{M}} \exists!_{(-A) \in \mathcal{M}}\big(A + (-A) = O = (-A) + A\big)$

(1) $A + (-A) = [a_{i,j} - a_{i,j}] = O = [-a_{i,j} + a_{i,j}] = (-A) + A$

(2) $A + (-A_1) = O = A + (-A_2) \;\blacksquare\; -A_1 = -A_2 \;\blacksquare\; A_1 = A_2$

$MulAssoc := \forall_{A,B,C \in \mathcal{M}}\big((A * B) * C = A * (B * C)\big)$

(1) $(A * B) * C = \left[\sum_{k_1=1}^{p_1}(a_{i,k_1} b_{k_1,j})\right] * C = \left[\sum_{k_2=1}^{p_2}\left(\sum_{k_1=1}^{p_1}(a_{i,k_1} b_{k_1,k_2}) c_{k_2,j}\right)\right] = \left[\sum_{k_2=1}^{p_2} \sum_{k_1=1}^{p_1}(a_{i,k_1} b_{k_1,k_2} c_{k_2,j})\right] = \ldots$

(2) $\ldots \left[\sum_{k_1=1}^{p_1} \sum_{k_2=1}^{p_2}(a_{i,k_1} b_{k_1,k_2} c_{k_2,j})\right] = \left[\sum_{k_1=1}^{p_1}\left(a_{i,k_1} \sum_{k_2=1}^{p_2}(b_{k_1,k_2} c_{k_2,j})\right)\right] = \ldots = A * (B * C)$

$MulId := \forall_{A : Square[A,n]}(A * I_n = A = I_n * A)$

(1) $A * I_n = \left[\sum_{k=1}^{n}\left(a_{i,k}\left(\begin{cases} 1 & k = j \\ 0 & k \neq j \end{cases}\right)\right)\right] = [a_{i,j}] = A$

(2) $TODO = A$

$ScalAssoc := \forall_{r,s\in\mathbb{R}}\forall_{A\in\mathcal{M}}\big(r(sA) = (rs)A = s(rA)\big)$

(1) $r(sA) = r[sa_{i,j}] = [rsa_{i,j}]$

(2) $(rs)A = [rsa_{i,j}]$

(3) $s(rA) = s[ra_{i,j}] = [sra_{i,j}] = [rsa_{i,j}]$

$TransCancel := \forall_{A\in\mathcal{M}}\big(A = (A^T)^T\big)$

(1) $A = [a_{i,j}] = [a_{j,i}]^T = ([a_{i,j}]^T)^T = (A^T)^T$

$ScalMulCom := \forall_{r\in\mathbb{R}}\forall_{A,B\in\mathcal{M}}\big((rA) * B = r(A * B) = A * (rB)\big)$

(1) $(rA) * B = [ra_{i,l}] * [b_{l,j}] = \left[\sum_{k=1}^{p}(ra_{i,k}b_{k,j})\right] = r(A * B)$

(2) $A * (rB) = [a_{i,l}] * [rb_{l,j}] = \left[\sum_{k=1}^{p}(a_{i,k}rb_{k,j})\right] = \left[\sum_{k=1}^{p}(ra_{i,k}b_{k,j})\right] = r(A * B)$

$ScalDistLeft := \forall_{r,s\in\mathbb{R}}\forall_{A\in\mathcal{M}}\big((r+s)A = rA + sA\big)$

(1) TODO

$ScalDistRight := \forall_{r\in\mathbb{R}}\forall_{A,B\in\mathcal{M}}\big(r(A+B) = rA + rB\big)$

(1) TODO

$MulDistRight := \forall_{A,B,C\in\mathcal{M}}\big((A+B) * C = A * C + B * C\big)$

(1) $(A+B) * C = [a_{i,j} + b_{i,j}] * C = \left[\sum_{k=1}^{p}\Big((a_{i,k} + b_{i,k})c_{k,j}\Big)\right] = \ \ldots$

(2) $\ldots \left[\sum_{k=1}^{p}(a_{i,k}c_{k,j} + b_{i,k}c_{k,j})\right] = \left[\sum_{k=1}^{p}(a_{i,k}c_{k,j})\right] + \left[\sum_{k=1}^{p}(b_{i,k}c_{k,j})\right] = A * C + B * C$

$MulDistLeft := \forall_{A,B,C\in\mathcal{M}}\big(C * (A+B) = C * A + C * B\big)$

(1) TODO

$TransAddDist := \forall_{A,B\in\mathcal{M}}\big((A+B)^T = A^T + B^T\big)$

(1) TODO

$TransMulDist := \forall_{A,B\in\mathcal{M}}\big((A * B)^T = B^T * A^T\big)$

(1) $(A * B)^T = \left[\sum_{k=1}^{p}(a_{i,k}b_{k,j})\right]^T = \left[\sum_{k=1}^{p}(a_{j,k}b_{k,i})\right] = \left[\sum_{k=1}^{p}(b_{k,i}a_{j,k})\right] = \left[\sum_{k=1}^{p}(b^T_{i,k}a^T_{k,j})\right] = B^T * A^T$

$Sym[A] := A = A^T$
$SkewSym[A] := A = -A^T$
$Invertible[A] := (Square[A,n]) \wedge \Big(\exists_{A^{-1}\in\mathcal{M}}(A * A^{-1} = I_n = A^{-1} * A)\Big)$

$SymGen := \forall_{A\in\mathcal{M}}(Sym[A + A^T])$

(1) $(A + A^T)^T = A^T + (A^T)^T = A^T + A = A + A^T$

$SkewSymGen := \forall_{A\in\mathcal{M}}(SkewSym[A - A^T])$

(1) $-(A - A^T)^T = -\big(A^T - (A^T)^T\big) = -(A^T - A) = (A - A^T)$

$SymDecomp := \forall_{A \in \mathcal{M}} \exists!_{B : Sym[B]} \exists!_{C : SkewSym[C]} (A = B + C)$

(1) $B := (1/2) * (A + A^T)\ ;\ C := (1/2) * (A - A^T)$

(2) $SymGen[B] \wedge SkewSymGen[C]$

(3) $A = (1/2) * (A + A^T) + (1/2) * (A - A^T) = B + C$

(4) $(1/2) * (A_1 + {A_1}^T) = (1/2) * (A_2 + {A_2}^T)\ \blacksquare\ A_1 = A_2$

(5) $(1/2) * (A_3 - {A_3}^T) = (1/2) * (A_4 - {A_4}^T)\ \blacksquare\ A_3 = A_4$

$InvId := \forall_{A : Invertible[A]} \left(\exists!_{A^{-1} \in \mathcal{M}} (A * A^{-1} = I_n = A^{-1} * A) \right)$

(1) ${A^{-1}}_1 = {A^{-1}}_1 * I_n = {A^{-1}}_1 * (A * {A^{-1}}_2) = ({A^{-1}}_1 * A) * {A^{-1}}_2 = I_n * {A^{-1}}_2 = {A^{-1}}_2$

$InvCancel := \forall_{A : Invertible[A]} \left((A^{-1})^{-1} = A \right)$

(1) $(A * A^{-1})^{-1} = {I_n}^{-1} = I_n$

(2) $(A^{-1})^{-1} * A^{-1} = I_n\ \blacksquare\ A^{-1})^{-1} = I_n * A = A$

$InvDist := \forall_{A : Invertible[A]} \forall_{B : Invertible[B]} \left((A * B)^{-1} = B^{-1} * A^{-1} \right)$

(1) $(A * B) * (A * B)^{-1} = I\ \blacksquare\ B * (A * B)^{-1} = A^{-1}\ \blacksquare\ (A * B)^{-1} = B^{-1} * A^{-1}$

$InvTrans := \forall_{A : Invertible[A]} \left((A^T)^{-1} = (A^{-1})^T \right)\ \blacksquare \Leftarrow$

(1) $A^T * (A^{-1})^T = (A^{-1} * A)^T = I^T = I\ \blacksquare\ (A^{-1})^T = (A^T)^{-1}$

3.2 Elementary Matrices on Invertibility and Systems of Linear Equations

$Sys[A, B] := (Matrix[A, m, n]) \wedge (Matrix[B, m, 1])$
$Sol[X, A, B] := (Sys[A, B]) \wedge (Matrix[X, n, 1]) \wedge (A * X = B)$
$ConsistentSys[A, B] := (Sys[A, B]) \wedge \exists_X (Sol[X, A, B])$
$TrivSol[X, A] := (Sol[X, A, O]) \wedge (X = O)$
$NonTrivSol[X, A] := (Sol[X, A, O]) \wedge (X \neq O)$

$HomoSysProps := (Sys[A, O]) \implies \ldots$

(1) $u_0 := O\ ;\ u_1 := choice(\{X \in \mathcal{M} | X \neq O\})\ ;\ k := choice(\mathbb{R})$

(2) $TrivSol[u_0, A]$

(3) $(NonTrivSol[u_1, A]) \implies (Sol[u_1 + ku_0])$

(4) $(TrivSol[\overrightarrow{X}, A]) \implies \left(TrivSol[LC(\overrightarrow{X}), A] \right)$

$ElemMat[E] := (E = Swap[I_n, i, j]) \vee \left(Scale_*(I_n, i, c) \right) \vee \left(Combine_*(I_n, i, c, j) \right)$
$ElemMatProd[E^*] := \exists_{\langle E \rangle} \left(\forall_{E_i \in E^*} (ElemMat[E_i]) \wedge \left(E^* = \Pi_{E_i \in E^*} (E_i) \right) \right)$
$RowEquiv[A, B] := \exists_{E^*} \left((ElemMatProd[E^*]) \wedge (B = E^* * A) \right)$

$ElemMatInv := \forall_{E \in \mathcal{M}} \left((ElemMat[E]) \implies (Invertible[E]) \right)$

(1) $E - RowSwap[E] \implies TODO\ ;\ E - RowScale_*(E) \implies TODO\ ;\ E - RowCombine_*(E) \implies TODO$

$ElemMatProdInv := \forall_{E^*} \left((ElemMatProd[E^*]) \implies (Invertible[E^*]) \right)$

(1) TODO

$RowEquivSys := \forall_{A,B,C,D,X \in \mathcal{M}} \left(\left((Sys[A, B]) \wedge (Sys[C, D]) \wedge (RowEquiv[[AB], [CD]]) \right) \implies (Sol[X, A, B] \iff Sol[X, C, D]) \right)$

(1) $\exists_{E^* : ElemMatProd[E^*]} ([CD] = E^* * [AB])$

(2) $(E^* * A = C) \land (E^* * B = D)$

(3) $Sol[Y, A, B] \implies \ldots$

(3.1) $A * Y = B$

(3.2) $C * Y = (E^* * A) * Y = E^* * (A * Y) = E^* * B = D \blacksquare Sol[Y, C, D]$

(4) $Sol[Y, A, B] \implies Sol[Y, C, D]$

(5) $\left(A = (E^*)^{-1} * C\right) \land \left(B = (E^*)^{-1} * D\right)$

(6) $Sol[Z, C, D] \implies \ldots$

(6.1) $C * Z = D$

(6.2) $A * Z = \left((E^*)^{-1} * C\right) * Z = (E^*)^{-1} * (C * Z) = (E^*)^{-1} * D = B$

(7) $Sol[Z, C, D] \implies Sol[Z, A, B]$

(8) $Sol[X, A, B] \iff Sol[X, C, D]$

$RowEquivHomoSysSol := \forall_{A,C,X \in \mathcal{M}}\Big((RowEquiv[A, C]) \implies \big((Sol[X, A, O]) \iff (Sol[X, C, O])\big)\Big)$

(1) Set $B = D = O$

$$RREF[A] := (A \in \mathcal{M}) \land \left(\begin{array}{ll} \text{All zero rows are at the bottom of the matrix.} & \land \\ \text{The leading entry after the first occurs to the right of the leading entry of the previous row.} & \land \\ \text{The leading entry in any nonzero row is 1.} & \land \\ \text{All entries in the column above and below a leading 1 are zero.} & \land \end{array}\right)$$

$GaussJordanElim := \forall_{A \in \mathcal{M}} \exists!_{B \in \mathcal{M}}\big((RREF[B]) \land (RowEquiv[A, B])\big)$

(1) Hit A with $ElemMat$'s until it becomes B

(2) $(B = E^* * A) \land (RREF[B])$

$HasZero[A] := \big(Matrix(A, m, n)\big) \land \big(\exists_{i \leq m}(A_{i,:} = O)\big)$

$HasZeroNonInvertible := \forall_{A \in \mathcal{M}}\big((HasZero[A]) \implies (\neg Invertible[A])\big)$

(1) $i := choice(\{i \leq m | A_{i,:} = O\})$

(2) $(B \in \mathcal{M}) \implies \ldots$

(2.1) $(A * B)_{i,:} = O \neq I_{ni,:} \blacksquare A * B \neq I_n$

(3) $(B \in \mathcal{M}) \implies (A * B \neq I_n) \blacksquare \forall_{B \in \mathcal{M}}(A * B \neq I_n) \blacksquare \neg Invertible[A]$

$InvIffRowEquivI := \forall_{A \in \mathcal{M}}\big((Invertible[A]) \iff (RowEquiv[A, I_n])\big)$

(1) $(Invertible[A]) \implies \ldots$

(1.1) $(RREF[B]) \land (RowEquiv[A, B])$

(1.2) $B = E^* * A$

(1.3) $(Invertible[E^*]) \land (Invertible[A]) \blacksquare Invertible[B]$

(1.4) $Invertible[B] \blacksquare \neg HasZero[B]$

(1.5) $(RREF[B]) \land (\neg HasZero[B]) \blacksquare B = I_n$

(1.6) $RowEquiv[A, I_n]$

(2) $(Invertible[A]) \implies (RowEquiv[A, I_n])$

(3) $(RowEquiv[A, I_n]) \implies \ldots$

(3.1) $I_n = E^* * A \blacksquare (E^*)^{-1} = A$

(3.2) $A^{-1} = E^*_{DescSort} \blacksquare Invertible[A]$

(4) $(RowEquiv[A, I_n]) \implies (Invertible[A])$

(5) $(Invertible[A]) \iff (RowEquiv[A, I_n])$

$RowEquivIIffTrivSol := \forall_{A \in \mathcal{M}}\Bigg((RowEquiv[A, I_n]) \iff \Big(\forall_X\big((X = O) \iff (Sol[X, A, O])\big)\Big)\Bigg)$

(1) $(RowEquiv[A, I_n]) \implies \ldots$

(1.1) $RowEquiv[A, I_n] \blacksquare Invertible[A]$

(1.2) $(Sol[X, A, O]) \implies \ldots$

(1.2.1) $A * X = O \blacksquare X = A^{-1} * O = O \blacksquare X = O$

(1.3) $(Sol[X, A, O]) \implies (X = O)$

(1.4) $(X = O) \implies (Sol[X, A, O])$

(1.5) $(X = O) \iff (Sol[X, A, O]) \blacksquare \forall_X\big((X = O) \iff (Sol[X, A, O])\big)$

(2) $(RowEquiv[A, I_n]) \implies \Big(\forall_X\big((X = O) \iff (Sol[X, A, O])\big)\Big)$

(3) $\Big(\forall_X\big((X = O) \iff (Sol[X, A, O])\big)\Big) \implies \ldots$

(3.1) $(RREF[B]) \wedge (RowEquiv[A, B])$

(3.2) $Sol[X, B, O]$

(3.3) $(B \neq I_n) \implies \ldots$

(3.3.1) $\Big(\exists_{Y \neq X}(Sol[Y, B, O])\Big)$

(3.3.2) $Sol[Y, A, O] \blacksquare Y = X$

(3.3.3) $(Y \neq X) \wedge (Y = X) \blacksquare \bot$

(3.4) $(B \neq I_n) \implies \bot \blacksquare B = I_n$

(3.5) $(RowEquiv[A, B]) \wedge (B = I_n) \blacksquare RowEquiv[A, I_n]$

(4) $\Big(\forall_X\big((X = O) \iff (Sol[X, A, O])\big)\Big) \implies (RowEquiv[A, I_n])$

(5) $(RowEquiv[A, I_n]) \iff \Big(\forall_X\big((X = O) \iff (Sol[X, A, O])\big)\Big)$

$$InvIffUniqSol := \forall_{A \in \mathcal{M}}\Big((Invertible[A]) \iff \big(\forall_{B \in \mathcal{M}} \exists!_{X \in \mathcal{M}}(Sol[X, A, B])\big)\Big)$$

(1) $(Invertible[A] \wedge B \in \mathcal{M}) \implies \ldots$

(1.1) $(Invertible[A]) \wedge (Sys[A, B])$

(1.2) $(X = A^{-1} * B) \iff (Sol[X, A, B]) \blacksquare \exists!_{X \in \mathcal{M}}(Sol[X, A, B])$

(2) $\big(\forall_{B \in \mathcal{M}} \exists!_{X \in \mathcal{M}}(Sol[X, A, B])\big) \implies \ldots$

(2.1) $X_i := choice(\{X_i | Sol[X_i, A, I_{n:,i}]\})$

(2.2) $A * [X_1 \ldots X_n] = [(A * X_1) \ldots (A * X_n)] = [I_{n:,1} \ldots I_{n:,n}] = I_n$

(2.3) $A^{-1} = [X_1 \ldots X_n]$

(3) $\big(\forall_{B \in \mathcal{M}} \exists!_{X \in \mathcal{M}}(Sol[X, A, B])\big) \implies (Invertible[A])$

$$SquareTheorems_4 := \forall_{A \in \mathcal{M}} \left(\begin{array}{l} (Invertible[A]) \iff \\ (RowEquiv[A, I_n]) \iff \\ \Big(\forall_X\big((X = O) \iff (Sol[X, A, O])\big)\Big) \iff \\ \big(\forall_{B \in \mathcal{M}} \exists!_{X \in \mathcal{M}}(Sol[X, A, B])\big) \end{array} \right)$$

3.3 Vector Spaces

$$VectorSpace[V, +, *] := \exists_{O \in V} \forall_{\alpha, \beta \in \mathbb{R}} \forall_{u, v, w \in V} \left(\begin{array}{l} (u + v \in V) \wedge (u + v = v + u) \wedge \big((u + v) + w = u + (v + w)\big) \wedge \\ (u + O = u) \wedge \Big(\exists_{-u \in V}\big(u + (-u) = O\big)\Big) \wedge \\ (\alpha * u \in V) \wedge \big(\alpha * (\beta * u) = (\alpha\beta) * u\big) \wedge (1 * u = u) \wedge \\ \big(\alpha * (u + v) = (\alpha * u) + (\alpha * v)\big) \wedge \big((\alpha + \beta) * u = (\alpha * u) + (\beta * u)\big) \end{array} \right)$$

$$ZeroVectorUniq := \forall_{O', v \in V}\big((v + O' = v) \implies (O' = O)\big)$$

(1) $O' = O' + O = O + O' = O \blacksquare O' = O$

$$AddInvUniq := \forall_{-v', v \in V}\big((v + -v' = O) \implies (-v' = -v)\big)$$

(1) $-v' = -v' + O = -v' + (v + -v) = (-v' + v) + -v = (v + -v') + -v = O + -v = -v \blacksquare -v' = -v$

$$AddInvGen := \forall_{v \in V}\big((-1) * v = -v\big)$$

(1) $v + (-1) * v = (1 - 1) * v = 0 * v = O$ ▮ $(-1) * v = -v$

$ZeroVectorGenLeft := \forall_{v \in V}(0 * v = O)$

(1) $0 * v = (0 + 0) * v = (0 * v) + (0 * v)$ ▮ $O = 0 * v$

$ZeroVectorGenRight := \forall_{r \in \mathbb{R}}(r * O = O)$

(1) $r * O = r * (O + O) = (r * O) + (r * O)$ ▮ $O = r * O$

$ZeroVectorEquiv := \forall_{r \in \mathbb{R}} \forall_{v \in V} \Big((r * v = O) \iff \big((v = O) \vee (r = 0)\big) \Big)$

(1) $(ZeroVectorGenLeft) \wedge (ZeroVectorGenRight)$ ▮ $\big((v = O) \vee (r = 0)\big) \implies (r * v = O))$

(2) $(r * v = O) \implies \ldots$

(2.1) $(r \neq 0) \implies \ldots$

(2.1.1) $r \neq 0$ ▮ $r^{-1} \in \mathbb{R}$

(2.1.2) $ZeroVectorGenRight$ ▮ $O = r^{-1} * O = r^{-1} * (r * v) = (r^{-1} r) * v = 1 * v = v$ ▮ $O = v$

(2.2) $(r \neq 0) \implies (v = O)$ ▮ $(r = 0) \vee (v = O)$

(3) $(r * v = O) \implies \big((r = 0) \vee (v = O)\big)$

(4) $(r * v = O) \iff \big((r = 0) \vee (v = O)\big)$

3.4 Subspaces and Special Subspaces

$Subspace[S, V, +, *] := (VectorSpace[V, +, *]) \wedge (S \subseteq V) \wedge (VectorSpace[S, +, *])$

$$SubspaceEquiv := \forall_{V,S} \left(\begin{array}{l} (VectorSpace[V, +, *]) \qquad\qquad \implies \\ \Big((Subspace[S, V, +, *]) \iff \Big((\emptyset \neq S \subseteq V) \wedge \big(\forall_{r,s \in S}(r + s \in S)\big) \wedge \big(\forall_{\alpha \in \mathbb{R}} \forall_{s \in S}(\alpha * s \in S)\big) \Big) \Big) \end{array} \right)$$

(1) $(Subspace[S, V, +, *]) \implies \ldots$

(1.1) $Subspace[S, V, +, *]$ ▮ $S \subseteq V$

(1.2) $VectorSpace[S, V, +, *]$ ▮ $\exists_{O \in V} \forall_{v \in V}(v + O = v)$ ▮ $O \in S$ ▮ $\emptyset \neq S$

(1.3) $(\emptyset \neq S) \wedge (S \subseteq V)$ ▮ $\emptyset \neq S \subseteq V$

(1.4) $VectorSpace[S, V, +, *]$ ▮ $\big(\forall_{r,s \in S}(r + s \in S)\big) \wedge \big(\forall_{\alpha \in \mathbb{R}} \forall_{s \in S}(\alpha * s \in S)\big)$

(1.5) $(\emptyset \neq S \subseteq V) \wedge \big(\forall_{r,s \in S}(r + s \in S)\big) \wedge \big(\forall_{\alpha \in \mathbb{R}} \forall_{s \in S}(\alpha * s \in S)\big)$

(2) $(Subspace[S, V, +, *]) \implies \Big((\emptyset \neq S \subseteq V) \wedge \big(\forall_{r,s \in S}(r + s \in S)\big) \wedge \big(\forall_{\alpha \in \mathbb{R}} \forall_{s \in S}(\alpha * s \in S)\big) \Big)$

(3) $\Big((\emptyset \neq S \subseteq V) \wedge \big(\forall_{r,s \in S}(r + s \in S)\big) \wedge \big(\forall_{\alpha \in \mathbb{R}} \forall_{s \in S}(\alpha * s \in S)\big) \Big) \implies \ldots$

(3.1) $\big((\emptyset \neq S) \wedge (\alpha, \beta \in \mathbb{R}) \wedge (u, v, w \in S)\big) \implies \ldots$

(3.1.1) $\emptyset \neq S$ ▮ $\exists_x (x \in V)$

(3.1.2) $(ZeroVectorGenLeft) \wedge \big(\forall_{\alpha \in \mathbb{R}} \forall_{s \in S}(\alpha * s \in S)\big) \wedge (x \in V)$ ▮ $O = 0 * x \in S$ ▮ $O \in S$

(3.1.3) $u, v \in V$ ▮ $u + v = v + u$

(3.1.4) $u, v, w \in V$ ▮ $(u + v) + w = u + (v + w)$

(3.1.5) $u \in V$ ▮ $u + O = u$

(3.1.6) $(AddInvGen) \wedge (u \in S)$ ▮ $(-1) * u = -u \in S$

(3.1.7) $u \in V$ ▮ $\alpha * (\beta * u) = (\alpha\beta) * u$

(3.1.8) $u \in V$ ▮ $1 * u = u$

(3.1.9) $u, v \in V$ ▮ $\alpha * (u + v) = (\alpha * u) + (\alpha * v)$

(3.1.10) $u \in V$ ▮ $(\alpha + \beta) * u = (\alpha * u) + (\beta * u)$

(4) $\Big((\emptyset \neq S) \wedge \big(\forall_{r,s \in S}(r + s \in S)\big) \wedge \big(\forall_{\alpha \in \mathbb{R}} \forall_{s \in S}(\alpha * s \in S)\big) \Big) \implies (Subspace[S, V, +, *])$

(5) $(Subspace[S, V, +, *]) \iff \Big((\emptyset \neq S) \wedge \big(\forall_{r,s \in S}(r + s \in S)\big) \wedge \big(\forall_{\alpha \in \mathbb{R}} \forall_{s \in S}(\alpha * s \in S)\big) \Big)$

$$SetSum[A+B,A,B,V,+,*] := (VectorSpace[V,+,*]) \land (A,B \subseteq V) \land \big(A+B = \{a+b | (a \in A) \land (b \in B)\}\big)$$

$$SumSubContains := \forall_{A,B,V}\left(\begin{array}{l} \big((Subspace[A,V,+,*]) \land (Subspace[B,V,+,*]) \land (SetSum[A+B,A,B,V,+,*])\big) \implies \\ \big((Subspace[A+B,V,+,*]) \land (A,B \subseteq A+B)\big) \end{array} \right)$$

(1) $(Subspace[A,V,+,*]) \land (Subspace[B,V,+,*]) \;\blacksquare\; (O \in A) \land (O \in B)$

(2) $(SetSum[A+B,A,B,V,+,*]) \land (O \in A) \land (O \in B) \;\blacksquare\; O = O + O \in A+B \;\blacksquare\; \emptyset \neq A+B$

(3) $(v \in A+B) \implies \ldots$

(3.1) $\exists_{a\in A}\exists_{b\in B}(v = a+b)$

(3.2) $(A \subseteq V) \land (B \subseteq V) \;\blacksquare\; a,b \in V$

(3.3) $VectorSpace[V,+,*] \;\blacksquare\; v = a+b \in V$

(4) $(v \in A+B) \implies (v \in V) \;\blacksquare\; A+B \subseteq V$

(5) $(\emptyset \neq A+B) \land (A+B \subseteq V) \;\blacksquare\; \emptyset \neq A+B \subseteq V$

(6) $(u,v \in A+B) \implies \ldots$

(6.1) $\big(\exists_{a_1\in A}\exists_{b_1\in B}(u = a_1+b_1)\big) \land \big(\exists_{a_2\in A}\exists_{b_2\in B}(v = a_2+b_2)\big)$

(6.2) $u+v = (a_1+b_1)+(a_2+b_2) = (a_1+a_2)+(b_1+b_2)$

(6.3) $(a_1+a_2 \in A) \land (b_1+b_2 \in B) \;\blacksquare\; u+v \in A+B$

(7) $(u,v \in A+B) \implies (u+v \in A+B) \;\blacksquare\; \forall_{u,v\in A+B}(u+v \in A+B)$

(8) $\big((r \in \mathbb{R}) \land (v \in A+B)\big) \implies \ldots$

(8.1) $\exists_{a\in A}\exists_{b\in B}(v = a+b)$

(8.2) $r*v = r*(a+b) = r*a + r*b$

(8.3) $(r*a \in A) \land (r*b) \in B \;\blacksquare\; r*v \in A+B$

(9) $\big((r \in \mathbb{R}) \land (v \in A+B)\big) \implies (r*v \in A+B) \;\blacksquare\; \forall_{r\in\mathbb{R}}\forall_{v\in A+B}(r*v \in A+B)$

(10) $(SubspaceEquiv) \land (\emptyset \neq A+B \subseteq V) \land \big(\forall_{u,v\in A+B}(u+v \in A+B)\big) \land \big(\forall_{r\in\mathbb{R}}\forall_{v\in A+B}(r*v \in A+B)\big) \;\blacksquare\; Subspace[A+B,V,+,*]$

(11) $(O \in B) \land \big(\forall_{a\in A}(a+O) = a\big) \;\blacksquare\; A \subseteq A+B$

(12) $(O \in A) \land \big(\forall_{b\in B}(b+O) = b\big) \;\blacksquare\; B \subseteq A+B$

(13) $(A \subseteq A+B) \land (B \subseteq A+B) \;\blacksquare\; A,B \subseteq A+B$

(14) $(Subspace[A+B,V,+,*]) \land (A,B \subseteq A+B)$

$$SumSubMinContains := \forall_{A,B,V}\left(\begin{array}{l} \big((Subspace[A,V,+,*]) \land (Subspace[B,V,+,*]) \land (SetSum[A+B,A,B,V,+,*])\big) \implies \\ \Big(\forall_C\big((Subspace[C,V,+,*]) \land (A,B \subseteq C)\big) \implies (A+B \subseteq C)\Big) \end{array} \right)$$

(1) $SumSub \;\blacksquare\; (A,B \subseteq A+B) \land (Subspace[A+B,V,+,*])$

(2) $\big((Subspace[C,V,+,*]) \land (A,B \subseteq C)\big) \implies \ldots$

(2.1) $(s \in A+B) \implies \ldots$

(2.1.1) $\exists_{a\in A}\exists_{b\in B}(s = a+b)$

(2.1.2) $(A,B \subseteq C) \;\blacksquare\; a,b \in C$

(2.1.3) $(VectorSpace[C,V,+,*]) \land (a,b \in C) \;\blacksquare\; s = a+b \in C$

(2.2) $(s \in A+B) \implies (s \in C) \;\blacksquare\; A+B \subseteq C$

(3) $\big((Subspace[C,V,+,*]) \land (A,B \subseteq C)\big) \implies (A+B \subseteq C)$

$$DirSum[A\oplus B,A,B,V,+,*] := \left(\begin{array}{l} (Subspace[A,V,+,*]) \quad \land \quad (Subspace[B,V,+,*]) \quad \land \\ (SetSum[A+B,A,B,V,+,*]) \land \big(\forall_{s\in A+B}\exists!_{\langle a,b\rangle\in A\times B}(s = a+b)\big) \end{array} \right)$$

$$DirSumEquiv := \forall_{A,B,V}\left(\begin{array}{l} \big((Subspace[A,V,+,*]) \land (Subspace[B,V,+,*]) \land (SetSum[A+B,A,B,V,+,*])\big) \implies \\ \Big((DirSum[A\oplus B,A,B,V,+,*]) \iff \big(\exists!_{\langle a,b\rangle\in A\times B}(O = a+b)\big)\Big) \end{array} \right)$$

(1) $(DirSum[A\oplus B,A,B,V,+,*]) \implies \ldots$

(1.1) $(Subspace[A,V,+,*]) \land (Subspace[B,V,+,*]) \;\blacksquare\; (O \in A) \land (O \in B)$

(1.2) $(SubSum[A \oplus B, A, B, V, +, *]) \wedge (O \in A) \wedge (O \in B) \;\blacksquare\; O = O + O \in A \oplus B$

(1.3) $(DirSum[A \oplus B, A, B, V, +, *]) \wedge (O \in A \oplus B) \;\blacksquare\; \exists!_{\langle a,b\rangle \in A\times B}(O = a + b)$

(2) $(DirSum[A \oplus B, A, B, V, +, *]) \implies \left(\exists!_{\langle a,b\rangle \in A\times B}(O = a + b)\right)$

(3) $\left(\exists!_{\langle a,b\rangle \in A\times B}(O = a + b)\right) \implies \ldots$

(3.1) $(s \in A \oplus B) \implies \ldots$

(3.1.1) $\left(\exists_{\langle a,b\rangle \in A\times B}(s = a + b)\right)$

(3.1.2) $\left((s = a_1 + b_1) \wedge (s = a_2 + b_2)\right) \implies \ldots$

(3.1.2.1) $O = s - s = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$

(3.1.2.2) $(Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *]) \;\blacksquare\; (a_1 - a_2 \in A) \wedge (b_1 - b_2 \in B)$

(3.1.2.3) $\left((a_1 - a_2 \neq O) \vee (b_1 - b_2 \neq O)\right) \implies \left(\neg\exists!_{\langle a,b\rangle \in A\times B}(O = a + b)\right) \implies \bot$

(3.1.2.4) $(a_1 - a_2 = O) \wedge (b_1 - b_2 = O) \;\blacksquare\; \langle a_1, b_1\rangle = \langle a_2, b_2\rangle$

(3.1.3) $\left((s = a_1 + b_1) \wedge (s = a_2 + b_2)\right) \implies \langle a_1, b_1\rangle = \langle a_2, b_2\rangle$

(3.1.4) $\forall_{\langle a_1,b_1\rangle,\langle a_2,b_2\rangle \in A\times B}\Big(\left((s = a_1 + b_1) \wedge (s = a_2 + b_2)\right) \implies (\langle a_1, b_1\rangle = \langle a_2, b_2\rangle)\Big)$

(3.1.5) $\exists_{\langle a,b\rangle \in A\times B}(s = a + b) \wedge \forall_{\langle a_1,b_1\rangle,\langle a_2,b_2\rangle \in A\times B}\Big(\left((s = a_1 + b_1) \wedge (s = a_2 + b_2)\right) \implies (\langle a_1, b_1\rangle = \langle a_2, b_2\rangle)\Big) \;\blacksquare\; \exists!_{\langle a,b\rangle \in A\times B}(s = a + b)$

(3.2) $(s \in A + B) \implies \exists!_{\langle a,b\rangle \in A\times B}(s = a + b) \;\blacksquare\; \forall_{s \in A+B}\exists!_{\langle a,b\rangle \in A\times B}(s = a + b) \;\blacksquare\; DirSum[A \oplus B, A, B, V, +, *]$

(4) $\left(\exists!_{\langle a,b\rangle \in A\times B}(O = a + b)\right) \implies (DirSum[A \oplus B, A, B, V, +, *])$

(5) $(DirSum[A \oplus B, A, B, V, +, *]) \iff \left(\exists!_{\langle a,b\rangle \in A\times B}(O = a + b)\right)$

$$DirSumSubspace := \forall_{A,B,V}\left(\begin{array}{l} ((Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *]) \wedge (SetSum[A + B, A, B, V, +, *])) \implies \\ ((DirSum[A \oplus B, A, B, V, +, *]) \iff (A \cap B = \{O\})) \end{array}\right)$$

(1) $(DirSum[A \oplus B, A, B, V, +, *]) \implies \ldots$

(1.1) $(v \in A \cap B) \implies \ldots$

(1.1.1) $(v \in A \cap B) \wedge (VectorSpace[B, +, *]) \;\blacksquare\; (v \in A) \wedge (v \in B) \;\blacksquare\; (v \in A) \wedge (-v \in B)$

(1.1.2) $(v \in A) \wedge (-v \in B) \;\blacksquare\; v + (-v) = O \in A + B$

(1.1.3) $DirSum[A \oplus B, A, B, V, +, *] \;\blacksquare\; \exists!_{\langle a,b\rangle \in A\times B}(O = a + b)$

(1.1.4) $(v \neq O) \implies \left(\neg\exists!_{\langle a,b\rangle \in A\times B}(O = a + b)\right) \implies \bot \;\blacksquare\; v = O$

(1.2) $(v \in A \cap B) \implies (v = O) \;\blacksquare\; A + B \subseteq \{O\}$

(1.3) $(v = O) \implies \ldots$

(1.3.1) $(Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *]) \;\blacksquare\; (O \in A) \wedge (O \in B) \;\blacksquare\; v = O \in A \cup B$

(1.4) $(v = O) \implies (v \in A \cap B) \;\blacksquare\; \{O\} \subseteq A \cap B$

(1.5) $(A + B \subseteq \{O\}) \wedge (\{O\} \subseteq A \cap B) \;\blacksquare\; A \cap B = \{O\}$

(2) $(DirSum[A \oplus B, A, B, V, +, *]) \implies (A \cap B = \{O\})$

(3) $(A \cap B = \{O\}) \implies \ldots$

(3.1) $(O \in A) \wedge (O \in B) \wedge (O = O + O \in A + B) \;\blacksquare\; \exists_{\langle a,b\rangle \in A\times B}(O = a + b)$

(3.2) $\left((\langle a_1, b_1\rangle, \langle a_2, b_2\rangle \in A \times B) \wedge (O = a_1 + b_1) \wedge (O = a_2 + b_2)\right) \implies \ldots$

(3.2.1) $(O = a_1 + b_1) \wedge (O = a_2 + b_2) \;\blacksquare\; (a_1 = -b_1) \wedge (a_2 = -b_2)$

(3.2.2) $VectorSpace[B, +, *] \;\blacksquare\; -b_1, -b_2 \in B$

(3.2.3) $(a_1 \in A) \wedge (a_1 = -b_1 \in B) \;\blacksquare\; a_1 \in A \cap B \;\blacksquare\; a_1 = O \;\blacksquare\; a_1 = b_1 = O$

(3.2.4) $(a_2 \in A) \wedge (a_2 = -b_2 \in B) \;\blacksquare\; a_2 \in A \cap B \;\blacksquare\; a_2 = O \;\blacksquare\; a_2 = b_2 = O$

(3.2.5) $\langle a_1, b_1\rangle = \langle O, O\rangle = \langle a_2, b_2\rangle$

(3.3) $\left((\langle a_1, b_1\rangle, \langle a_2, b_2\rangle \in A \times B) \wedge (O = a_1 + b_1) \wedge (O = a_2 + b_2)\right) \implies (\langle a_1, b_1\rangle = \langle a_2, b_2\rangle)$

(3.4) $\forall_{\langle a_1,b_1\rangle,\langle a_2,b_2\rangle \in A\times B}\Big(\left((O = a_1 + b_1) \wedge (O = a_2 + b_2)\right) \implies (\langle a_1, b_1\rangle = \langle a_2, b_2\rangle)\Big)$

(3.5) $\left(\exists_{\langle a,b\rangle \in A\times B}(O = a + b)\right) \wedge \left(\forall_{\langle a_1,b_1\rangle,\langle a_2,b_2\rangle \in A\times B}\Big(\left((O = a_1 + b_1) \wedge (O = a_2 + b_2)\right) \implies (\langle a_1, b_1\rangle = \langle a_2, b_2\rangle)\Big)\right)$

(3.6) $\left(\exists!_{\langle a,b\rangle \in A\times B}(O = a + b)\right) \wedge (DirSumEquiv) \blacksquare DirSum[A \oplus B, A, B, V, +, *]$

(4) $(A \cap B = \{O\}) \implies (DirSum[A \oplus B, A, B, V, +, *])$

(5) $(DirSum[A \oplus B, A, B, V, +, *]) \iff (A \cap B = \{O\})$

$NullSpace[N, A, m, n] := (Matrix[A, m, n]) \wedge (N = \{x \in \mathbb{R}^n | A * x = O\})$
$RowSpace[R, A, m, n] := (Matrix[A, m, n]) \wedge (R = \{x^T * A \in \mathbb{R}^n | x \in \mathbb{R}^m\})$
$ColSpace[C, A, m, n] := (Matrix[A, m, n]) \wedge (C = \{A * x \in \mathbb{R}^m | x \in \mathbb{R}^n\})$

$NullSubspace := (NullSpace[N, A, m, n]) \implies (Subspace[N, \mathbb{R}^n, +, *])$

(1) TODO

$RowSubspace := (RowSpace[R, A, m, n]) \implies (Subspace[R, \mathbb{R}^n, +, *])$

(1) TODO

$ColSubspace := (ColSpace[C, A, m, n]) \implies (Subspace[C, \mathbb{R}^m, +, *])$

(1) TODO

3.5 Linear Combination, Linear Span, Linear Independence

$LinComb[c, U, K, V, +, *] := (VectorSpace[V, +, *]) \wedge (n \in \mathbb{N}) \wedge (U \in V^n) \wedge (K \in \mathbb{R}^n) \wedge \left(c = \sum_{i=1}^n (k_i * u_i)\right)$

$$LinSpan[S', S, V, +, *] := \left(\begin{array}{c} (VectorSpace[V, +, *]) \wedge (S \in V^n) \wedge \left((S = \emptyset) \implies (S' = \{O\})\right) \quad \wedge \\ \left((S \neq \emptyset) \implies \left(S' = \{c \in V | (K \in \mathbb{R}^n) \wedge (LinComb[c, S, K, V, +, *])\}\right)\right) \end{array} \right)$$

$LinSpanSubContains := \forall_{S', S, V}\left((LinSpan[S', S, V, +, *]) \implies \left((Subspace[S', V, +, *]) \wedge (S \subseteq S')\right)\right)$

(1) $(S = \emptyset) \implies \ldots$

(1.1) $LinSpan[S', S, V, +, *] \blacksquare S' = \{O\}$

(1.2) $Subspace[\{O\}, V, +, *] \blacksquare Subspace[S', V, +, *]$

(1.3) $S = \emptyset \subseteq \{O\} = S' \blacksquare S \subseteq S'$

(1.4) $(Subspace[S', V, +, *]) \wedge (S \subseteq S')$

(2) $(S = \emptyset) \implies \left((Subspace[S', V, +, *]) \wedge (S \subseteq S')\right)$

(3) $(S \neq \emptyset) \implies \ldots$

(3.1) $LinSpan[S', S, V, +, *] \blacksquare S' = \{c \in V | (K \in \mathbb{R}^n) \wedge (LinComb[c, S, K, V, +, *])\} \blacksquare S' \subseteq V$

(3.2) $(\{0\}^n \subseteq \mathbb{R}^n) \wedge (LinComb[O, S, \{0\}^n, V, +, *]) \blacksquare O \in S' \blacksquare \emptyset \neq S'$

(3.3) $(S' \subseteq V) \wedge (\emptyset \neq S') \blacksquare \emptyset \neq S' \subseteq V$

(3.4) $(a, b \in S') \implies \ldots$

(3.4.1) $\left(\exists_{K_a \in \mathbb{R}^n}(LinComb[a, S, K_a, V, +, *])\right) \wedge \left(\exists_{K_b \in \mathbb{R}^n}(LinComb[b, S, K_b, V, +, *])\right) \blacksquare \left(a = \sum_{i=1}^n (k_{ai} * s_i)\right) \wedge \left(b = \sum_{i=1}^n (k_{bi} * s_i)\right)$

(3.4.2) $a + b = \sum_{i=1}^n (k_{ai} * s_i) + \sum_{i=1}^n (k_{bi} * s_i) = \sum_{i=1}^n \left((k_{ai} + k_{bi}) * s_i\right) \blacksquare a + b = \sum_{i=1}^n \left((k_{ai} + k_{bi}) * s_i\right)$

(3.4.3) $\langle k_{ai} + k_{bi} | i \in \mathbb{N}_{1,n}\rangle \in \mathbb{R}^n$

(3.4.4) $\left(a + b = \sum_{i=1}^n \left((k_{ai} + k_{bi}) * s_i\right)\right) \wedge (\langle k_{ai} + k_{bi} | i \in \mathbb{N}_{1,n}\rangle \in \mathbb{R}^n) \;\ldots$

(3.4.5) $\ldots \exists_{M \in \mathbb{N}^n}\left(a + b = \sum_{i=1}^n (m_i * s_i)\right) \blacksquare \exists_{M \in \mathbb{N}^n}(LinComb[a + b, S, M, V, +, *]) \blacksquare a + b \in S'$

(3.5) $(a, b \in S') \implies (a + b \in S') \blacksquare \forall_{a,b \in S'}(a + b \in S')$

(3.6) $\left((r \in \mathbb{R}) \wedge (u \in S')\right) \implies \ldots$

(3.6.1) $\exists_{K \in \mathbb{R}^n}(LinComb[u, S, K, V, +, *]) \blacksquare u = \sum_{i=1}^n (k_i * s_i)$

(3.6.2) $r * u = r * \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^n \left(r * (k_i * s_i)\right) = \sum_{i=1}^n (rk_i) * s_i \blacksquare r * u = \sum_{i=1}^n (rk_i) * s_i$

(3.6.3) $\langle rk_i \in \mathbb{R} | i \in \mathbb{N}_{1,n} \rangle \in \mathbb{R}^n$

(3.6.4) $\left(r * u = \sum_{i=1}^{n}(rk_i) * s_i)\right) \wedge (\langle rk_i \in \mathbb{R} | i \in \mathbb{N}_{1,n} \rangle \in \mathbb{R}^n) \blacksquare \exists_{M \in \mathbb{R}^n}\left(r * u = \sum_{i=1}^{n}(m_i * s_i)\right)$

(3.6.5) $\exists_{M \in \mathbb{R}^n}(LinComb[r * u, S, M, V, +, *]) \blacksquare r * u \in S'$

(3.7) $\left((r \in \mathbb{R}) \wedge (u \in S')\right) \implies (r * u \in S') \blacksquare \forall_{r \in \mathbb{R}} \forall_{u \in S'}(r * u \in S')$

(3.8) $(SubspaceEquiv) \wedge (\emptyset \neq S' \subseteq V) \wedge \left(\forall_{a,b \in S'}(a + b \in S')\right) \wedge \left(\forall_{r \in \mathbb{R}} \forall_{u \in S'}(r * u \in S')\right) \blacksquare Subspace[S', V, +, *]$

(3.9) $(s_i \in S) \implies \ldots$

(3.9.1) $K_s := \left\langle \left(\begin{cases} 1 & j = i \\ 0 & j \neq i \end{cases} \right) | j \in \mathbb{N}_{1,n} \right\rangle \blacksquare (K_s \in \mathbb{R}^n) \wedge \left(\sum_{j=1}^{n}(k_{sj} * s_j) = s_i\right)$

(3.9.2) $\exists_{K \in \mathbb{R}^n}(LinComb[s_j, S, K, V, +, *]) \blacksquare s_j \in S'$

(3.10) $(s_i \in S) \implies (s_i \in S') \blacksquare S \subseteq S'$

(3.11) $(Subspace[S', V, +, *]) \wedge (S \subseteq S')$

(4) $(S \neq \emptyset) \implies \left((Subspace[S', V, +, *]) \wedge (S \subseteq S')\right)$

(5) $\left((S = \emptyset) \implies \left((Subspace[S', V, +, *]) \wedge (S \subseteq S')\right)\right) \wedge \left((S \neq \emptyset) \implies \left((Subspace[S', V, +, *]) \wedge (S \subseteq S')\right)\right) \ldots$

(6) $\ldots (Subspace[S', V, +, *]) \wedge (S \subseteq S')$

$$LinSpanSubMinContains := \forall_{S', S, V, +, *}\left((LinSpan[S', S, V, +, *]) \implies \left(\forall_W\left(((Subspace[W, V, +, *]) \wedge (S \subseteq W)) \implies (S' \subseteq W)\right)\right)\right)$$

(1) $(s' \in S') \implies \ldots$

(1.1) $\exists_{K \in \mathbb{R}^n}(LinComb[s', S, K, V, +, *]) \blacksquare s' = \sum_{i=1}^{n}(k_i * s_i)$

(1.2) $(S \subseteq W) \wedge (VectorSpace[W, V, +, *]) \blacksquare s' = \sum_{i=1}^{n}(k_i * s_i) \in W \blacksquare s' \in W$

(2) $(s' \in S') \implies (s' \in W) \blacksquare S' \subseteq W$

$Spans[S, V, +, *] := LinSpan[V, S, V, +, *]$
$FinDim[V, +, *] := \exists_{S \in V^n}(Spans[S, V, +, *])$

$$LinInd[S, V, +, *] := (VectorSpace[V, +, *]) \wedge (S \in V^n) \wedge \left((S \neq \emptyset) \implies \left(\forall_{K \in \mathbb{R}^n}\left((LinComb[O, S, K, V, +, *]) \implies (K = \{0\}^n)\right)\right)\right)$$

$ZeroDependent := (O \in S) \implies (\neg LinInd[S, V, +, *])$

(1) $O \in S \blacksquare \exists_{u_i \in S}(u_i = O) \blacksquare K := \left\langle \left(\begin{cases} 1 & u_i = O \\ 0 & u_i \neq O \end{cases} \right) | i \in \mathbb{N}_{1,n} \right\rangle \blacksquare \{O\}^n \neq K \in \mathbb{R}^n$

(2) $O = \sum_{i=1}^{n}(k_i * s_i) \blacksquare LinComb[O, S, K, V, +, *]$

(3) $(LinComb[O, S, K, V, +, *]) \wedge (\{O\}^n \neq K \in \mathbb{R}^n) \blacksquare \exists_{K \in \mathbb{R}^n}\left((LinComb[O, S, K, V, +, *]) \wedge (K \neq \{0\}^n)\right) \blacksquare \neg LinInd[S, V, +, *]$

$SingletonNonZeroIndependent := (v \neq O) \implies (LinInd[\langle v \rangle, V, +, *])$

(1) $\left((\langle r \rangle \in \mathbb{R}^1) \wedge (LinComb[O, \langle v \rangle, \langle r \rangle, V, +, *])\right) \implies \ldots$

(1.1) $(ZeroVectorEquiv) \wedge (r * v = O) \blacksquare (r * v = O) \iff \left((r = 0) \vee (v \neq O)\right)$

(1.2) $v \neq O \blacksquare r = 0$

(2) $\left((\langle r \rangle \in \mathbb{R}^1) \wedge (LinComb[O, \langle v \rangle, \langle r \rangle, V, +, *])\right) \implies (r = 0) \blacksquare \forall_{r \in \mathbb{R}}\left((LinComb[O, \langle v \rangle, \langle r \rangle, V, +, *]) \implies (r = 0)\right)$

(3) $LinInd[\langle v \rangle, V, +, *]$

$$SubIndependent := \forall_{V, A, B}\left(\begin{array}{l} \left((VectorSpace[V, +, *]) \wedge (A \subseteq B) \wedge (A \in V^n) \wedge (B \in V^m)\right) \implies \\ \left((LinInd[B, V, +, *]) \implies (LinInd[A, V, +, *])\right) \end{array} \right)$$

(1) $\left((K \in \mathbb{R}^n) \wedge (LinComb[O, A, K, V, +, *])\right) \implies \ldots$

(1.1) $n \leq m \;\blacksquare\; L := \langle \left(\begin{cases} k_j & j \leq n \\ 0 & j > n \end{cases} \middle| j \in \mathbb{N}_{1,m} \right) \rangle \;\blacksquare\; L \in \mathbb{R}^m$

(1.2) $A \subseteq B \;\blacksquare\; \forall_{j \in \mathbb{N}_{1,n}} (a_j = b_j) \;\blacksquare\; \sum_{i=1}^{n} (k_i * a_i)) = \sum_{j=1}^{m} (l_j * b_j))$

(1.3) $LinComb[O, A, K, V, +, *] \;\blacksquare\; O = \sum_{i=1}^{n} (k_i * a_i) = \sum_{j=1}^{m} (l_j * b_j)) \;\blacksquare\; LinComb[O, B, L, V, +, *]$

(1.4) $(LinInd[B, V, +, *]) \wedge (LinComb[O, B, L, V, +, *]) \;\blacksquare\; L = \{0\}^m \;\blacksquare\; K = \{0\}^n$

(2) $\big((K \in \mathbb{R}^n) \wedge (LinComb[O, A, K, V, +, *])\big) \implies (K = \{0\}^n) \;\blacksquare\; LinInd[A, V, +, *]$

$SuperDependent := \forall_{V,A,B} \Big(\big((VectorSpace[V, +, *]) \wedge (A \subseteq B \subseteq V)\big) \implies \big((\neg LinInd[A, V, +, *]) \implies (\neg LinInd[B, V, +, *])\big) \Big)$

(1) $\neg LinInd[A, V, +, *] \;\blacksquare\; \exists_K \big((LinComb[O, A, K, V, +, *]) \wedge (K \neq \{0\}^n)\big)$

(2) $n \leq m \;\blacksquare\; L := \langle \left(\begin{cases} k_j & j \leq n \\ 0 & j > n \end{cases} \middle| j \in \mathbb{N}_{1,m} \right) \rangle \;\blacksquare\; L \in \mathbb{R}^m$

(3) $A \subseteq B \;\blacksquare\; \forall_{j \in \mathbb{N}_{1,n}} (a_j = b_j) \;\blacksquare\; \sum_{i=1}^{n} (k_i * a_i)) = \sum_{j=1}^{m} (l_j * b_j))$

(4) $LinComb[O, A, K, V, +, *] \;\blacksquare\; LinComb[O, B, L, V, +, *]$

(5) $K \neq \{0\}^n \;\blacksquare\; L \neq \{0\}^m$

(6) $\exists_L \big((LinComb[O, B, L, V, +, *]) \wedge (L \neq \{0\}^m)\big) \;\blacksquare\; \neg LinInd[B, V, +, *]$

$LinDepProp := \forall_{S,V} \Big((\neg LinInd[S, V, +, *]) \implies \big(\exists_{s_j \in S} \exists_{K \in \mathbb{R}^{n-1}} (LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])\big) \Big)$

(1) $\neg LinInd[S, V, +, *] \;\blacksquare\; \exists_{K \in \mathbb{R}^n} \big((LinComb[O, S, K, V, +, *]) \wedge (K \neq \{0\}^n)\big)$

(2) $K \neq \{0\}^n \;\blacksquare\; \exists_{j \in \mathbb{N}_{1,n}} \Big((k_j \neq 0) \wedge \big(\forall_{i \in \mathbb{N}_{j+1,n}} (k_i = 0)\big) \Big) \;\ldots$

(3) $\ldots \sum_{i=1}^{n} (k_i * s_i) = \sum_{i=1}^{j} (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j \;\blacksquare\; \sum_{i=1}^{n} (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j$

(4) $(LinComb[O, S, K, V, +, *]) \wedge \Big(\sum_{i=1}^{n} (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j\Big) \;\blacksquare\; O = \sum_{i=1}^{n} (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j$

(5) $s_j = (-1/k_j) \sum_{i=1}^{j-1} (k_i * s_i) = \sum_{i=1}^{j-1} \Big((-k_i/k_j) * s_i\Big) \;\blacksquare\; s_j = \sum_{i=1}^{j-1} \Big((-k_i/k_j) * s_i\Big)$

(6) $\exists_{K \in \mathbb{R}^{n-1}} (LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])$

$LinDepPropCorollary := \forall_{P,S,V} \Big(\big((\neg LinInd[S, V, +, *]) \wedge (LinSpan[P, S, V, +, *])\big) \implies \big(\exists_{s_j \in S} (LinSpan[P, S \setminus \{s_j\}, V, +, *])\big) \Big)$

(1) $LinDepProp \;\blacksquare\; \exists_{s_j \in S} \exists_{K \in \mathbb{R}^{n-1}} (LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])$

(2) $\forall_{u \in P} \Big(\big(\exists_{K_1} (LinComb[u, S, K_1, V, +, *])\big) \implies \big(\exists_{K_2} (LinComb[u, S \setminus \{s_j\}, K_2, V, +, *])\big) \Big) \;\blacksquare\; LinSpan[P, S \setminus \{s_j\}, V, +, *]$

$LinIndEquiv := \forall_{S,V} \Big((LinInd[S, V, +, *]) \iff \big(\forall_{s_j \in S} \forall_{K \in \mathbb{R}^{n-1}} (\neg LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])\big) \Big)$

(1) $LinDepProp \;\blacksquare\; (\neg LinInd[S, V, +, *]) \implies \big(\exists_{s_j \in S} \exists_{K \in \mathbb{R}^{n-1}} (LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])\big) \;\ldots$

(2) $\ldots \big(\forall_{s_j \in S} \forall_{K \in \mathbb{R}^{n-1}} (\neg LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])\big) \implies (LinInd[S, V, +, *])$

(3) $\big(\exists_{s_j \in S} \exists_{K \in \mathbb{R}^{n-1}} (LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])\big) \implies \ldots$

(3.1) $L := \langle \left(\begin{cases} k_i & i \neq j \\ -1 & i = j \end{cases} \middle| i \in \mathbb{N}_{1,n} \right) \rangle \;\blacksquare\; (L \in \mathbb{R}^n) \wedge (L \neq \{0\}^n)$

(3.2) $LinComb[s_j, S \setminus \{s_j\}, K, V, +, *] \;\blacksquare\; \ldots \;\blacksquare\; \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j = \sum_{i=1}^{j-1} (k_i * s_i) + - \sum_{i=1}^{j-1} (k_i * s_i) = O \;\ldots$

(3.3) $\ldots LinComb[O, S, L, V, +, *]$

(3.4) $(LinComb[O, S, L, V, +, *]) \wedge (L \neq \{0\}^n) \;\blacksquare\; \exists_{L \in \mathbb{R}^n} \big((LinComb[O, S, L, V, +, *]) \wedge (L \neq \{0\}^n)\big) \;\blacksquare\; (\neg LinInd[S, V, +, *])$

(4) $\big(\exists_{s_j \in S} \exists_{K \in \mathbb{R}^{n-1}} (LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])\big) \implies (\neg LinInd[S, V, +, *])$

(5) $(LinInd[S,V,+,*]) \implies \Big(\forall_{s_j\in S}\forall_{K\in\mathbb{R}^{n-1}}(\neg LinComb[s_j, S\setminus\{s_j\}, K, V, +, *])\Big)$

(6) $(LinInd[S,V,+,*]) \iff \Big(\forall_{s_j\in S}\forall_{K\in\mathbb{R}^{n-1}}(\neg LinComb[s_j, S\setminus\{s_j\}, K, V, +, *])\Big)$

$LinIndSuperspace := \forall_{U,V}\Bigg((Subspace[U,V]) \implies \Big(\forall_W\big((LinInd[W,U,+,*]) \implies (LinInd[W,V,+,*])\big)\Big)\Bigg)$

(1) $(\neg LinInd[W,V,+,*]) \implies \ldots$

(1.1) $\exists_{j\in W}(LinComb[j, W\setminus\{j\},+,*]) \;\blacksquare\; \neg LinInd[W,U,+,*]$

(1.2) $(LinInd[W,U,+,*]) \wedge (\neg LinInd[W,U,+,*]) \;\blacksquare\; \bot$

(2) $(\neg LinInd[W,V,+,*]) \implies \bot \;\blacksquare\; LinInd[W,V,+,*]$

3.6 Bases and Dimensions

$Basis[S,V,+,*] := (Spans[S,V,+,*]) \wedge (LinInd[S,V,+,*])$

$BasisEquiv := \forall_{S,V}\big((Basis[S,V,+,*]) \iff (\forall_{v\in V}\exists!_{K\in\mathbb{R}^n}(LinComb[v,S,K,V,+,*])\big)$

(1) $(Basis[S,V,+,*]) \implies \ldots$

(1.1) $(v\in V) \implies \ldots$

(1.1.1) $Basis[S,V,+,*] \;\blacksquare\; Spans[V,S,+,*] \;\blacksquare\; \exists_{K\in\mathbb{R}^n}(LinComb[v,S,K,V,+,*])$

(1.1.2) $\big((K_1,K_2\in\mathbb{R}^n)\wedge(LinComb[v,S,K_1,V,+,*])\wedge(LinComb[v,S,K_2,V,+,*])\big) \implies \ldots$

(1.1.2.1) $\big(v = \sum(k_{1i} * s_i)\big) \wedge \big(v = \sum(k_{2i} * s_i)\big)$

(1.1.2.2) $O = v - v = \sum(k_{1i} * s_i) - \sum(k_{2i} * s_i) = \sum\big((k_{1i} - k_{2i}) * s_i\big)$

(1.1.2.3) $L := \langle k_{1i} - k_{2i} | i \in \mathbb{N}_{i=1}^n\rangle \in \mathbb{R}^n$

(1.1.2.4) $(LinInd[S,V,+,*]) \wedge (LinComb[O,S,L,V,+,*]) \;\blacksquare\; L = \{0\}^n \;\blacksquare\; K_2 = K_1$

(1.1.3) $\big((K_1,K_2\in\mathbb{R}^n)\wedge(LinComb[v,S,K_1,V,+,*])\wedge(LinComb[v,S,K_2,V,+,*])\big) \implies (K_1 = K_2)$

(1.1.4) $\forall_{K_1,K_2\in\mathbb{R}^n}\big((LinComb[v,S,K_1,V,+,*])\wedge(LinComb[v,S,K_2,V,+,*]) \implies (K_1 = K_2)\big)$

(1.1.5) $\exists!_{K\in\mathbb{R}^n}(LinComb[v,S,K,V,+,*])$

(1.2) $(v\in V) \implies \big(\exists!_{K\in\mathbb{R}^n}(LinComb[v,S,K,V,+,*])\big)$

(2) $(Basis[S,V,+,*]) \implies \big(\forall_{v\in V}\exists!_{K\in\mathbb{R}^n}(LinComb[v,S,K,V,+,*])\big)$

(3) $\big(\forall_{v\in V}\exists!_{K\in\mathbb{R}^n}(LinComb[v,S,K,V,+,*])\big) \implies \ldots$

(3.1) $\forall_{v\in V}\exists!_{K\in\mathbb{R}^n}(LinComb[v,S,K,V,+,*]) \;\blacksquare\; \forall_{v\in V}\exists_{K\in\mathbb{R}^n}(LinComb[v,S,K,V,+,*]) \;\blacksquare\; Spans[S,V,+,*]$

(3.2) $O\in V \;\blacksquare\; \exists!_{K\in\mathbb{R}^n}(LinComb[O,S,K,V,+,*])$

(3.3) $(K \neq \{0\}^n) \implies \big(\neg\exists!_{K\in\mathbb{R}^n}(LinComb[O,S,K,V,+,*])\big) \implies \bot \;\blacksquare\; K = \{0\}^n$

(3.4) $\big(\exists!_{K\in\mathbb{R}^n}(LinComb[O,S,K,V,+,*])\big) \wedge (K = \{0\}^n) \;\blacksquare\; LinInd[S,V,+,*]$

(3.5) $(Spans[S,V,+,*]) \wedge (LinInd[S,V,+,*]) \;\blacksquare\; Basis[S,V,+,*]$

(4) $\big(\forall_{v\in V}\exists!_{K\in\mathbb{R}^n}(LinComb[v,S,K,V,+,*])\big) \implies (Basis[S,V,+,*])$

$SpanReduceBasis := \forall_{S,V}\Bigg((Spans[S,V,+,*]) \implies \Big(\exists_B\big((B\subseteq S)\wedge(Basis[B,V,+,*])\big)\Big)\Bigg)$

(1) $LinDepPropCorollary \;\blacksquare\; \exists_B\big((B\subseteq S)\wedge(LinInd[B,V,+,*])\wedge(Spans[B,V,+,*])\big) \;\blacksquare\; \exists_B\big((B\subseteq S)\wedge(Basis[B,V,+,*])\big)$

(2) TODO - formalize removing latter entries first

$FinDimBasis := \forall_V\Big((FinDim[V,+,*]) \implies \big(\exists_B(Basis[B,V,+,*])\big)\Big)$

(1) $FinDim[V,+,*] \;\blacksquare\; \exists_{S\in V^n}(Spans[S,V,+,*])$

(2) $(SpanReduceBasis) \wedge (Spans[S,V,+,*]) \;\blacksquare\; \exists_B(Basis[B,V,+,*])$

$LinIndExpandBasis := \forall_{L,V}\Bigg((LinInd[L,V,+,*]) \implies \Big(\exists_B\big((L\subseteq B)\wedge(Basis[B,V,+,*])\big)\Big)\Bigg)$

(1) $FinDimBasis \blacksquare \exists_C(Basis[C,V,+,*])$

(2) $S := L \cup C$

(3) $Basis[C,V,+,*] \blacksquare Spans[C,V,+,*] \blacksquare Spans[S,V,+,*]$

(4) $SpanReduceBasis \blacksquare \Big(\exists_B\big((B \subseteq S) \wedge (Basis[B,V,+,*])\big)\Big) \wedge (L \subseteq B)$

$SpanLinIndLength := \forall_{S,T,V}\Big(\big((Span[S,V,+,*]) \wedge (LinInd[T,V,+,*])\big) \implies (|T| \leq |S|)\Big)$

(1) $\big((Span[S,V,+,*]) \wedge (|T| > |S|)\big) \implies \ldots$

  (1.1) $Span[S,V,+,*] \blacksquare \forall_{i\in\mathbb{N}_{1,|H|}}\exists_{K_i\mathbb{R}^{|S|}}(LinComb[t_i,S,K_iV,+,*])$

  (1.2) $|H| > |S| \blacksquare \exists_{L\in\mathbb{R}^{|H|-1}}(LinComb[t_{|H|},T \setminus \{t_{|H|}\},L,V,+,*])$

  (1.3) $L = -1 * K \blacksquare \big(\sum(K+L) = O\big) \wedge (K + L \neq \{0\}^{|T|}) \blacksquare \neg LinInd[T,V,+,*]$

  (1.4) TODO - tidy up

(2) $\big((Span[S,V,+,*]) \wedge (|T| > |S|)\big) \implies (\neg LinInd[T,V,+,*]) \blacksquare \big((Span[S,V,+,*]) \wedge (LinInd[T,V,+,*])\big) \implies (|T| \leq |S|)$

$BasisLength := \forall_{S,T,V}\Big(\big((Basis[S,V,+,*]) \wedge (Basis[T,V,+,*])\big) \implies (|T| = |S|)\Big)$

(1) $(Span[T,V,+,*]) \wedge (LinInd[S,V,+,*]) \blacksquare |S| \leq |T|$

(2) $(Span[S,V,+,*]) \wedge (LinInd[T,V,+,*]) \blacksquare |T| \leq |S|$

(3) $(|S| \leq |T|) \wedge (|T| \leq |S|) \blacksquare |T| = |S|$

$Dim[d,V,+,*] := \big((V = \{O\}) \implies (d = 0)\big) \wedge \Bigg((V \neq \{O\}) \implies \Big(\big(\exists_B(Basis[B,V,+,*])\big) \wedge (d = |B|)\Big)\Bigg)$

$LinIndLengthDim := \forall_{U,V}\Big(\big((LinInd[U,V,+,*]) \wedge (Dim[|U|,V,+,*])\big) \implies (Basis[U,V,+,*])\Big)$

(1) $(LinIndExpandBasis) \wedge (LinInd[U,V,+,*]) \blacksquare \exists_B\big((U \subseteq B) \wedge (Basis[B,V,+,*])\big)$

(2) $(BasisLength) \wedge (Dim[|U|,V,+,*]) \wedge (Basis[B,V,+,*]) \blacksquare |B| = |U| \blacksquare B = U \blacksquare Basis[U,V,+,*]$

$SpanLengthDim := \forall_{U,V}\Big(\big((Spans[U,V,+,*]) \wedge (Dim[|U|,V,+,*])\big) \implies (Basis[U,V,+,*])\Big)$

(1) $(SpanReduceBasis) \wedge (Spans[U,V,+,*]) \blacksquare \exists_B\big((B \subseteq U) \wedge (Basis[B,V,+,*])\big)$

(2) $(BasisLength) \wedge (Dim[|U|,V,+,*]) \wedge (Basis[B,V,+,*]) \blacksquare |B| = |U| \blacksquare B = U \blacksquare Basis[U,V,+,*]$

$LinDepLengthDim := \forall_{U,V}\Big(\big((U \subseteq V) \wedge (|U| > Dim[V])\big) \implies (\neg LinInd[U,V,+,*])\Big)$

(1) Contrapositive of $BasisLinearIndCard$

(2) TODO - cleanup

$NonSpanLengthDim := \forall_{U,V}\Big(\big((U \subseteq V) \wedge (|U| < Dim[V])\big) \implies (\neg Spans[U,V,+,*])\Big)$

(1) Suppose $Spans[U,V,+,*]$, $B = SpanReduceBasis[U]$ to form a basis, $(|B| \leq |U| < Dim[V]) \wedge |B| = Dim[V] \blacksquare \bot$

(2) $\neg Spans[U,V,+,*]$

(3) TODO - cleanup

3.7 Rank

$Nullity[n,A] := (NullSpace[N,A]) \wedge (Dim[n,N,+,*])$
$Rank[r,A,m,n] := (Matrix[A,m,n]) \wedge (RowSpace[R,A,m,n]) \wedge (Dim[r,R,A,+,*])$

$RowRankEqColRank := \forall_A(TODO)$

(1) TODO

$RankNullity := \forall_A\big((Matrix[A,m,n]) \implies (Rank[A] + Nullity[A] = n)\big)$

(1) TODO

$$RankInv := \forall_A\Big((Matrix[A,m,n]) \implies \big((Rank[A]=n) \iff (Inv[A])\big)\Big)$$

(1) TODO

$$RankNonTrivialSol := \Big(\exists_X\big((A*X=O)\wedge(X\neq O)\big)\Big) \iff (Rank[A]<n)$$

(1) TODO

$$RankUniqueSol := \big(\forall_{B\in\mathcal{M}}\exists!_{X\in\mathcal{M}}(Sol[X,A,B])\big) \iff (Rank[A]=n)$$

(1) TODO

$$SquareTheorems_8 := \forall_{A\in\mathcal{M}}\left(\begin{array}{ll} (Invertible[A]) & \iff \\ (RowEquiv[A,I_n]) & \iff \\ \Big(\forall_X\big((X=O)\iff(Sol[X,A,O])\big)\Big) & \iff \\ \big(\forall_{B\in\mathcal{M}}\exists!_{X\in\mathcal{M}}(Sol[X,A,B])\big) & \iff \\ (Rank[A]=n) & \iff \\ (Nullity[A]=0) & \iff \\ \big(\text{The rows form a linearly independent set of vectors (to get full rank)}\big) & \iff \\ \big(\text{The columns form a linearly independent set of vectors (to get full rank)}\big) & \iff \end{array}\right)$$

3.8 Linear Transformations

$$LinTrans[L,V,+_v,*_v,W,+_w,*_w] := \left(\begin{array}{c}(Function[f,V,W])\wedge(VectorSpace[V,+_v,*_v])\wedge(VectorSpace[W,+_w,*_w])\wedge \\ \Big(\forall_{\alpha,\beta\in V}\big(L(\alpha+_v\beta)=L(\alpha)+_w L(\beta)\big)\Big) \wedge \Big(\forall_{r\in\mathbb{R}}\forall_{\alpha\in V}\big(L(r*_v\alpha)=r*_w L(\alpha)\big)\Big)\end{array}\right)$$

$$LinOp[L,V,+_v,*_v] := LinTrans[L,V,+_v,*_v,V,+_v,*_v]$$

$$\mathcal{L}[V,W] := \{L|LinTrans[L,V,+_v,*_v,W,+_w,*_w]\}$$

$$ZeroMapsToZero := \forall_{L,V,W}\Big((LinTrans[L,V,+_v,*_v,W,+_w,*_w]) \implies \big(L(O_v)=O_w\big)\Big)$$

(1) $L(O_v)=L(O_v+_v O_v)=L(O_v)+_w L(O_v)$

(2) $O_w=L(O_v)-L(O_v)=L(O_v)$

$$SplitAddInv := \forall_{L,V,W}\Bigg((LinTrans[L,V,+_v,*_v,W,+_w,*_w]) \implies \Big(\forall_{\alpha,\beta\in V}\big(L(\alpha-_v\beta)=L(\alpha)-_w L(\beta)\big)\Big)\Bigg)$$

(1) $L(\alpha-\beta)=L\big(\alpha+(-\beta)\big)=L(\alpha)+L(-\beta)=L(\alpha)+(-1)*L(\beta)=L(\alpha)-L(\beta)$

$$UniqBasisLT := \forall_{V,W}\left(\begin{array}{l}\big((VectorSpace[V,+_v,*_v])\wedge(VectorSpace[W,+_w,*_w])\wedge(Basis[A,V,+_v,*_v])\wedge(Basis[B,W,+_w,*_w])\big) \implies \\ \Bigg(\exists!_T\bigg((LinTrans[T,V,+_v,*_v,W,+_w,*_w])\wedge\Big(\forall_{i\in\mathbb{N}_{1,n}}\big(T(a_i)=b_i\big)\Big)\bigg)\Bigg)\end{array}\right)$$

(1) $T\big(\sum_{i=1}^n(k_i*a_i)\big) := \sum_{i=1}^n(k_i*b_i)$

(2) $(i\in\mathbb{N}_{1,n}) \implies \ldots$

(2.1) $L := \langle\left(\begin{cases}1 & j=i\\ 0 & j\neq i\end{cases}\right)|j\in\mathbb{N}_{1,n}\rangle$ ▮ $L\in\mathbb{R}^n$

(2.2) $T(a_i)=T\big(\sum_{i=1}^n(l_i*a_i)\big)=\sum_{i=1}^n(l_i*b_i)=b_i$ ▮ $T(a_i)=b_i$

(3) $(i\in\mathbb{N}_{1,n}) \implies \big(T(a_i)=b_i\big)$ ▮ $\forall_{i\in\mathbb{N}_{1,n}}\big(T(a_i)=b_i\big)$

(4) $(BasisEquiv)\wedge(Basis[A,V,+_v,*_v])$ ▮ $\forall_{v\in V}\exists!_{K\in\mathbb{R}^n}(LinComb[v,A,K,V,+,*])$ ...

(5) $\ldots\forall_{v_1,v_2\in V}\Big((v_1=v_2) \implies \big(T(v_1)=T(v_2)\big)\Big)$ ▮ $Function[T,V,W]$

(6) $(\alpha,\beta\in V) \implies \ldots$

(6.1) $\Big(\exists_{K_\alpha}(LinComb[\alpha,A,K_\alpha,V,+_v,*_v])\Big)\wedge\Big(\exists_{K_\beta}(LinComb[\beta,A,K_\beta,V,+_v,*_v])\Big)$ ▮ $\big(\alpha=\sum_{i=1}^n(k_{\alpha i}*a_i)\big)\wedge\Big(\beta=\sum_{i=1}^n(k_{\beta_i}*a_i)\Big)$

(6.2) $T(\alpha+\beta) = T\Big(\sum_{i=1}^n (k_{\alpha i} * a_i) + \sum_{i=1}^n (k_{\beta_i} * a_i)\Big) = T\Big(\sum_{i=1}^n \big((k_{\alpha i} + k_{\beta_i}) * a_i\big)\Big)) = \sum_{i=1}^n \big((k_{\alpha i}+k_{\beta_i}) * b_i\big) = \ \dots$

(6.3) $\dots \sum_{i=1}^n (k_{\alpha i} * b_i) + \sum_{i=1}^n (k_{\beta_i} * b_i) = T\big(\sum_{i=1}^n (k_{\alpha i} * a_i)\big) + T\Big(\sum_{i=1}^n (k_{\beta_i} * a_i)\Big) = T(\alpha)+T(\beta)$

(7) $(\alpha,\beta\in V) \implies \big(L(\alpha +_v \beta) = L(\alpha) +_w L(\beta)\big) \blacksquare \forall_{\alpha,\beta\in V}\big(L(\alpha +_v \beta) = L(\alpha) +_w L(\beta)\big)$

(8) $\big((r\in\mathbb{R})\wedge(\alpha\in V)\big) \implies \dots$

(8.1) $\exists_K(LinComb[\alpha, A, K, V, +_v, *_v]) \blacksquare \alpha = \sum_{i=1}^n (k_i * a_i)$

(8.2) $L(r *_v \alpha) = L\big(r *_v \sum_{i=1}^n (k_i *_v a_i)\big) = L\Big(\sum_{i=1}^n \big((rk_i) *_v a_i\big)\Big) = \ \dots$

(8.3) $\dots \sum_{i=1}^n \big((rk_i) *_w b_i\big) = r *_w \sum_{i=1}^n (k_i *_w b_i) = r *_w L\big(\sum_{i=1}^n (k_i *_v a_i)\big) = r *_w L(\alpha)$

(9) $\big((r\in\mathbb{R})\wedge(\alpha\in V)\big) \implies \big(L(r *_v \alpha) = r *_w L(\alpha)\big) \blacksquare \forall_{r\in\mathbb{R}}\forall_{\alpha\in V}\big(L(r *_v \alpha) = r *_w L(\alpha)\big)$

(10) $\Big(\forall_{i\in\mathbb{N}_{1,n}}\big(T(a_i)=b_i\big)\Big)\wedge(Function[T,V,W])\wedge\Big(\forall_{\alpha,\beta\in V}\big(L(\alpha +_v \beta) = L(\alpha) +_w L(\beta)\big)\Big)\wedge\Big(\forall_{r\in\mathbb{R}}\forall_{\alpha\in V}\big(L(r *_v \alpha) = r *_w L(\alpha)\big)\Big)\wedge\ \dots$

(11) $\dots(VectorSpace[V,+_v,*_v])\wedge(VectorSpace[W,+_w,*_w]) \blacksquare \Big(\forall_{i\in\mathbb{N}_{1,n}}\big(T(a_i)=b_i\big)\Big)\wedge(LinTrans[T,V,+_v,*_v,W,+_w,*_w])$

(12) $\bigg(\Big(\forall_{i\in\mathbb{N}_{1,n}}\big(T_2(a_i)=b_i\big)\Big)\wedge(LinTrans[T_2,V,+_v,*_v,W,+_w,*_w])\bigg) \implies \dots$

(12.1) $\forall_{i\in\mathbb{N}_{1,n}}\big(T_2(a_i)=b_i\big) \blacksquare \forall_{i\in\mathbb{N}_{1,n}}\big(T_2(c_i * a_i) = c_i * b_i\big) \blacksquare T_2\big(\sum_{i=1}^n (c_i * a_i)\big) = \sum_{i=1}^n (c_i * b_i) \blacksquare T_2 = T$

(13) $\bigg(\Big(\forall_{i\in\mathbb{N}_{1,n}}\big(T_2(a_i)=b_i\big)\Big)\wedge(LinTrans[T_2,V,+_v,*_v,W,+_w,*_w])\bigg) \implies (T_2 = T)$

$+_{\mathcal{L}}[S+T,S,T] := (S+T)(v) = S(v)+T(v)$
$*_{\mathcal{L}}\ [r*T,r,T] := (r*T)(v) = r*\big(T(v)\big)$
$LTVectorSpace := \forall_{V,W}(VectorSpace[\mathcal{L}[V,W],+_{\mathcal{L}},*_{\mathcal{L}}])$

(1) TODO

$*_{\mathcal{L}}\ [S*T,S,T] := (S*T)(v) = S\big(T(v)\big)$
$LTProdProperties := (associativity)\wedge(identity)\wedge(distributive)$

(1) TODO

$Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w] := (LinTrans[L,V,+_v,*_v,W,+_w,*_w])\wedge\big(ker_L = \{\alpha\in V \mid L(\alpha)=O_w\}\big)$

$KerSubspace := \forall_{L,V,W}\big((Ker[ker_L,L,V,+_v,*_v,W,+_w,*_w]) \implies (Subspace[ker_L,V,+_v,*_v])\big)$

(1) $ZeroMapsToZero \blacksquare L(O_v)=O_w \blacksquare O_v\in ker_L \blacksquare \emptyset\neq ker_L \blacksquare \emptyset\neq ker_L\subseteq V$

(2) $(\alpha,\beta\in ker_L)\implies\dots$

(2.1) $\big(L(\alpha)=O_w\big)\wedge\big(L(\beta)=O_w\big)$

(2.2) $L(\alpha+\beta)=L(\alpha)+L(\beta)=O_w+O_w=O_w \blacksquare L(\alpha+\beta)\in ker_L$

(3) $(\alpha,\beta\in ker_L)\implies(\alpha+\beta\in ker_L) \blacksquare \forall_{\alpha,\beta\in ker_L}(\alpha+\beta\in ker_L)$

(4) $\big((r\in\mathbb{R})\wedge(\alpha\in ker_L)\big)\implies\dots$

(4.1) $L(\alpha)=O_w \blacksquare L(r*\alpha)=r*L(\alpha)=r*O_w=O_w \blacksquare r*\alpha\in ker_L$

(5) $\big((r\in\mathbb{R})\wedge(\alpha\in ker_L)\big)\implies(r*\alpha\in ker_L) \blacksquare \forall_{r\in\mathbb{R}}\forall_{\alpha\in ker_L}(r*\alpha\in ker_L)$

(6) $(SubspaceEquiv)\wedge(\emptyset\neq ker_L\subseteq V)\wedge\Big(\forall_{\alpha,\beta\in ker_L}(\alpha+\beta\in ker_L)\Big)\wedge\Big(\forall_{r\in\mathbb{R}}\forall_{\alpha\in ker_L}(r*\alpha\in ker_L)\Big) \blacksquare Subspace[ker_L,V,+_v,*_v]$

$Rng[rng_L,L,V,+_v,*_v,W,+_w,*_w] := (LinTrans[L,V,+_v,*_v,W,+_w,*_w])\wedge\Big(rng_L = \{\beta\in W \mid \exists_{\alpha\in V}\big(\beta=L(\alpha)\big)\}\Big)$

$RangeSubspace := \forall_{L,V,W}\big((Ran[rng_L,L,V,+_v,*_v,W,+_w,*_w]) \implies (Subspace[rng_L,W,+_w,*_w])\big)$

(1) $ZeroMapsToZero \blacksquare O_w = L(O_v) \blacksquare \exists_{\alpha\in V}\big(O_w=L(\alpha)\big) \blacksquare O_w\in rng_L \blacksquare \emptyset\neq rng_L \blacksquare \emptyset\neq rng_L\subseteq W$

(2) $(\alpha,\beta\in rng_L)\implies\dots$

(2.1) $\left(\exists_{u\in V}\left(\alpha = L(u)\right)\right) \wedge \left(\exists_{v\in V}\left(\beta = L(v)\right)\right)$

(2.2) $\alpha + \beta = L(u) + L(v) = L(u+v) \;\blacksquare\; \exists_{w\in V}\left(\alpha+\beta = L(w)\right) \;\blacksquare\; \alpha+\beta \in rng_L$

(3) $(\alpha, \beta \in rng_L) \implies (\alpha+\beta \in rng_L) \;\blacksquare\; \forall_{\alpha,\beta\in rng_L}(\alpha+\beta \in rng_L)$

(4) $\left((r \in \mathbb{R}) \wedge (\alpha \in rng_L)\right) \implies \ldots$

(4.1) $\exists_{v\in V}\left(\alpha = L(v)\right) \;\blacksquare\; L(r * v) = r * L(v) = r * \alpha \;\blacksquare\; \exists_{w\in V}\left(r*\alpha = L(w)\right) \;\blacksquare\; r*\alpha \in rng_L$

(5) $\left((r \in \mathbb{R}) \wedge (\alpha \in rng_L)\right) \implies (r*\alpha \in rng_L) \;\blacksquare\; \forall_{r\in\mathbb{R}}\forall_{\alpha\in rng_L}(r*\alpha \in rng_L)$

(6) $(SubspaceEquiv) \wedge (\emptyset \neq rng_L \subseteq W) \wedge \left(\forall_{\alpha,\beta\in rng_L}(\alpha+\beta \in rng_L)\right) \wedge \left(\forall_{r\in\mathbb{R}}\forall_{\alpha\in rng_L}(r*\alpha \in rng_L)\right) \;\blacksquare\; Subspace[rng_L, W, +_w, *_w]$

$KerInjective := \forall_{L,V,W}\left((Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w]) \implies \left((Injective[L,V,W]) \iff (ker_L = \{O_v\})\right)\right)$

(1) $(Injective[L,V,W]) \implies \ldots$

(1.1) $ZeroMapsToZero \;\blacksquare\; L(O_v) = O_w$

(1.2) $O_v \in ker_L \;\blacksquare\; \{O_v\} \subseteq ker_L$

(1.3) $(v \in ker_L) \implies \ldots$

(1.3.1) $L(v) = O_w$

(1.3.2) $(Injective[L,V,W]) \wedge \left(L(O_v) = O_w\right) \;\blacksquare\; O_v = v$

(1.4) $(v \in ker_L) \implies (v = O_v) \;\blacksquare\; ker_L \subseteq \{O_v\}$

(1.5) $(\{O_v\} \subseteq ker_L) \wedge (ker_L \subseteq \{O_v\}) \;\blacksquare\; ker_L = \{O_v\}$

(2) $(Injective[L,V,W]) \implies (ker_L = \{O_v\})$

(3) $(ker_L = \{O_v\}) \implies \ldots$

(3.1) $\left((u, v \in V) \wedge \left(L(u) = L(v)\right)\right) \implies \ldots$

(3.1.1) $O_w = L(u) - L(v) = L(u-v) \;\blacksquare\; u - v \in ker_L$

(3.1.2) $ker_L = \{O_v\} \;\blacksquare\; u - v = O_v \;\blacksquare\; u = v$

(3.2) $\left((u, v \in V) \wedge \left(L(u) = L(v)\right)\right) \implies (u = v) \;\blacksquare\; \forall_{u,v\in V}\left(\left(L(u) = L(v)\right) \implies (u = v)\right) \;\blacksquare\; Injective[L,V,W]$

(4) $(ker_L = \{O_v\}) \implies (Injective[L,V,W])$

(5) $(Injective[L,V,W]) \iff (ker_L = \{O_v\})$

$RankNullityLT := \forall_{L,V,W}\left((LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \implies (Dim[V] = Dim[ker_L] + Dim[rng_L])\right)$

(1) $KerSubspace \;\blacksquare\; \left(\exists_U(Basis[U, ker_L, +_v, *_v])\right) \wedge (Dim[ker_L] = |U|)$

(2) $(LinIndSuperspace) \wedge (LinInd[U, ker_L, +_v, *_v]) \;\blacksquare\; LinInd[U, V, +_v, *_v]$

(3) $(LinIndExpandBasis) \wedge (LinInd[U, V, +_v, *_v]) \;\blacksquare\; \left(\exists_B\left((U \subseteq B) \wedge (Basis[B, V, +_v, *_v])\right)\right) \wedge (Dim[V] = |B|)$

(4) $U \subseteq B \;\blacksquare\; \exists_T(B = U \cup T)$

(5) $(w \in rng_L) \implies \ldots$

(5.1) $\exists_{v\in V}\left(w = L(v)\right)$

(5.2) $(Basis[B, V, +_v, *_v]) \wedge (B = U \cup T) \;\blacksquare\; \exists_{K\in\mathbb{R}^{|B|}}\left(v = \sum_{i=1}^{|B|}(k_i * b_i) = \sum_{i=1}^{|U|}(k_i * u_i) + \sum_{i=1}^{|T|}(k_{|U|+i} * t_i)\right)$

(5.3) $w = L(v) = L\left(\sum_{i=1}^{|U|}(k_i * u_i) + \sum_{i=1}^{|T|}(k_{|U|+i} * t_i)\right) = L\left(\sum_{i=1}^{|U|}(k_i * u_i)\right) + L\left(\sum_{i=1}^{|T|}(k_{|U|+i} * t_i)\right) = \;\ldots$

(5.4) $O + L\left(\sum_{i=1}^{|T|}(k_{|U|+i} * t_i)\right) = \sum_{i=1}^{|T|}\left(L(k_{|U|+i} * t_i)\right) = \sum_{i=1}^{|T|}\left(k_{|U|+i} * L(t_i)\right) \;\blacksquare\; \exists_K\left(LinComb[w, L(T), K, W, +, *]\right)$

(6) $(w \in rng_L) \implies \left(\exists_L\left(LinComb[w, L(T), L, W, +, *]\right)\right) \;\blacksquare\; Spans[L(T), rng_L, W, +, *]$

(7) $\left((K \in \mathbb{R}^n) \wedge \left(LinComb[O_w, L(T), K, W, +_w, *_w]\right)\right) \implies \ldots$

(7.1) $O_w = \sum_{i=1}^{n}\left(k_i * L(t_i)\right) = L\left(\sum_{i=1}^{n}(k_i * t_i)\right) \;\blacksquare\; \sum_{i=1}^{n}(k_i * t_i) \in ker_L$

(7.2) $(Basis[U, ker_L, +_v, *_v]) \wedge \left(\sum_{i=1}^{n}(k_i * t_i) \in ker_L\right) \;\blacksquare\; \exists_{D\in\mathbb{R}^m}\left(\sum_{i=1}^{n}(k_i * t_i) = \sum_{i=1}^{m}(d_i * u_i)\right)$

(7.3) $Basis[B] \;\blacksquare\; LinInd[B] \;\blacksquare\; LinInd[U \cup T] \;\blacksquare\; \forall_{s_j\in U\cup T}\forall_{K\in\mathbb{R}^{n-1}}(\neg LinComb[s_j, U \cup T \setminus \{s_j\}, K, V, +, *])$

(7.4) $\left(\sum_{i=1}^{n}(k_i * t_i) = \sum_{i=1}^{m}(d_i * u_i)\right) \wedge \left(\forall_{s_j\in U\cup T}\forall_{K\in\mathbb{R}^{n-1}}(\neg LinComb[s_j, U \cup T \setminus \{s_j\}, K, V, +, *])\right) \;\blacksquare\; (D = \{O\}) \wedge (K = \{O\})$

(8) $\left((K \in \mathbb{R}^n) \land \left(LinComb[O_w, L(T), K, W, +_w, *_w]\right)\right) \implies (K = \{O\})$ ▮ $LinInd[L(T), W, +_w, *_w]$

(9) $(SubIndependent) \land \left(LinInd[L(T), W, +_w, *_w]\right)$ ▮ $LinInd[L(T), rng_L, +_w, *_w]$

(10) $\left(Spans[L(T), rng_L, W, +, *]\right) \land \left(LinInd[L(T), rng_L, +_w, *_w]\right)$ ▮ $Basis[L(T), rng_L, +_w, *_w]$ ▮ $Dim[rng_L] = |L(T)| = |T|$

(11) $B = U \cup T$ ▮ $|B| = |U| + |T|$ ▮ $Dim[V] = Dim[ker_L] + Dim[rng_L]$

$$InjectiveSurjectiveEqualDim := \forall_{T,V,W}\left(\begin{array}{l}\left((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \land (Dim[V] = Dim[W]) \land (Injective[T, V, W])\right) \implies \\ (Surjective[T, V, W])\end{array}\right)$$

(1) $(KerInjective) \land (Injective[T, V, W])$ ▮ $ker_T = \{O\}$ ▮ $Dim[ker_T] = 0$

(2) $(RankNullityLT) \land (Dim[ker_T] = 0)$ ▮ $Dim[V] = Dim[ker_T] + Dim[rng_T] = Dim[rng_T]$ ▮ $Dim[V] = Dim[rng_T]$

(3) $(Dim[V] = Dim[W]) \land (Dim[V] = Dim[rng_T])$ ▮ $Dim[W] = Dim[rng_T]$

(4) $RangeSubspace$ ▮ $Subspace[rng_T, W, +_w, *_w]$

(5) $(Subspace[rng_T, W, +_w, *_w]) \land (Dim[W] = Dim[rng_T])$ ▮ $\exists_B\left((Basis[B, W, +_w, *_w]) \land (Basis[B, rng_T, +_w, *_w])\right)$

(6) $(Spans[W] = Spans[rng_T])$ ▮ $W = rng_T$ ▮ $Surjective[T, V, W]$

$$SurjectiveInjectiveEqualDim := \forall_{T,V,W}\left(\begin{array}{l}\left((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \land (Dim[V] = Dim[W]) \land (Surjective[T, V, W])\right) \implies \\ (Injective[T, V, W])\end{array}\right)$$

(1) $RankNullityLT$ ▮ $Dim[V] = Dim[ker_T] + Dim[rng_T]$

(2) $Surjective[T, V, W]$ ▮ $rng_T = W$ ▮ $Dim[rng_T] = Dim[W]$

(3) $(Dim[V] = Dim[W]) \land (Dim[V] = Dim[ker_T] + Dim[rng_T]) \land (Dim[rng_T] = Dim[W])$ ▮ $Dim[ker_T] + Dim[rng_T] = Dim[rng_T]$ ▮ $Dim[ker_T] = 0$ ▮ $ker_T = \{O\}$

(4) $(KerInjective) \land (er_T = \{O\})$ ▮ $Injective[T, V, W]$

$$SmallerMapNotInjective := \forall_{T,V,W}\left(\left((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \land (Dim[V] > Dim[W])\right) \implies (\neg Injective[T, V, W])\right)$$

(1) $(RankNullityLT) \land (Dim[W] \geq Dim[rng_T])$ ▮ $Dim[ker_T] = Dim[V] - Dim[rng_T] \geq Dim[V] - Dim[W] > 0$ ▮ $Dim[ker_T] \neq 0$

(2) $(KerInjective) \land (Dim[ker_T] \neq 0)$ ▮ $\neg Injective[T, V, W]$

$$LargerMapNotSurjective := \forall_{T,V,W}\left(\left((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \land (Dim[V] < Dim[W])\right) \implies (\neg Surjective[T, V, W])\right)$$

(1) $RankNullityLT$ ▮ $Dim[rng_T] = Dim[V] - Dim[ker_T] \leq Dim[V] < Dim[W]$

(2) $Dim[rng_T] < Dim[W]$ ▮ $Dim[rng_T] \neq Dim[W]$ ▮ $\neg Surjective[T, V, W]$

A linear transformation L : V -> W is one-to-one if and only if the image of every linearly independent set of vectors in V is linearly independent set of vectors in W .

(1) TODO

A homogeneous system of linear equations with more variables than equations has nonzero solutions.

(1) TODO

An inhomogeneous system of linear equations with more equations than variables has no solution for some choice of the constant terms.

(1) TODO

$$LTInv[L^{-1}, L, V, +_v, *_v, W, +_w, *_w] := \left(\begin{array}{lcr}(LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \land (LinTrans[L^{-1}, W, +_w, *_w, V, +_v, *_v]) \land & & \\ (L^{-1} \circ L = 1_v) & \land & (L \circ L^{-1} = 1_w)\end{array}\right)$$

$$LTInvUniq := \forall_{L_1^{-1}, L_2^{-1}}\left(\left((LTInv[L_1^{-1}, L, V, +_v, *_v, W, +_w, *_w]) \land (LTInv[L_2^{-1}, L, V, +_v, *_v, W, +_w, *_w])\right) \implies (L_1^{-1} = L_2^{-1})\right)$$

(1) $L_1^{-1} = L_1^{-1} \circ 1_w = L_1^{-1} \circ (L \circ L_2^{-1}) = (L_1^{-1} \circ L) \circ L_2^{-1} = 1_v \circ L_2^{-1} = L_2^{-1}$ ▮ $L_1^{-1} = L_2^{-1}$

$$LTInvertible[L, V, +_v, *_v, W, +_w, *_w] := \exists_{L^{-1}}(LTInv[L^{-1}, L, V, +_v, *_v, W, +_w, *_w])$$

$InvertibleBijectiveEquiv := \forall_L\Big((LTInvertible[L,V,+_v,*_v,W,+_w,*_w]) \iff \big((Injective[L,V,W]) \wedge (Surjective[L,V,W])\big)\Big)$

(1) $(LTInvertible[L,V,+_v,*_v,W,+_w,*_w]) \implies \ldots$

(1.1) $\exists_{L^{-1}}(LTInv[L^{-1},L,V,+_v,*_v,W,+_w,*_w])$

(1.2) $\big(L(u)=L(w)\big) \implies \ldots$

(1.2.1) $u = L^{-1}\big(L(u)\big) = L^{-1}\big(L(v)\big) = v \;\blacksquare\; u = v$

(1.3) $\big(L(u)=L(w)\big) \implies (u=w) \;\blacksquare\; \forall_{u,w}\Big(\big(L(u)=L(w)\big) \implies (u=w)\Big) \;\blacksquare\; Injective[L,V,W]$

(1.4) $(w \in W) \implies \ldots$

(1.4.1) $L^{-1}(w) \in V$

(1.4.2) $L \circ L^{-1} = 1_w \;\blacksquare\; L\Big(L^{-1}(w) = w\Big)$

(1.4.3) $\Big(L^{-1}(w) \in V\Big) \wedge \Big(L\Big(L^{-1}(w)=w\Big)\Big) \;\blacksquare\; \exists_{v\in V}\Big(w = \big(L(v)\big)\Big)$

(1.5) $(w \in W) \implies \Big(\exists_{v\in V}\Big(w = \big(L(v)\big)\Big)\Big) \;\blacksquare\; \forall_{w\in W}\exists_{v\in V}\big(w = L(v)\big) \;\blacksquare\; Surjective[L,V,W]$

(1.6) $(Injective[L,V,W]) \wedge (Surjective[L,V,W])$

(2) $(LTInvertible[L,V,+_v,*_v,W,+_w,*_w]) \implies \big((Injective[L,V,W]) \wedge (Surjective[L,V,W])\big)$

(3) $\big((Injective[L,V,W]) \wedge (Surjective[L,V,W])\big) \implies \ldots$

(3.1) $(Injective[L,V,W]) \wedge (Surjective[L,V,W]) \;\blacksquare\; \forall_{w\in W}\exists!_{v\in V}\big(w = L(v)\big)$

(3.2) $S := \{(w,v) \in W \times V | w = L(v)\}$

(3.3) $\Big(\forall_{w\in W}\exists!_{v\in V}\big(w = L(v)\big)\Big) \wedge \big(S = \{(w,v) \in W \times V | w = L(v)\}\big) \;\blacksquare\; Function[S,W,V]$

(3.4) $\Big(\forall_{v\in V}\Big(S\big(L(v)\big) = v\Big)\Big) \wedge \Big(\forall_{w\in W}\Big(L\big(S(w)\big) = w\Big)\Big)$

(3.5) $(w_1, w_2 \implies W) \implies \ldots$

(3.5.1) $(LinTrans[L,V,+_v,*_v,W,+_w,*_w]) \wedge \Big(\forall_{w\in W}\Big(L\big(S(w)\big) = w\Big)\Big) \;\blacksquare\; L\big(S(w_1)+S(w_2)\big) = L\big(S(w_1)\big) + L\big(S(w_2)\big) = w_1 + w_2$

(3.5.2) $\Big(\forall_{w\in W}\Big(L\big(S(w)\big) = w\Big)\Big) \wedge (w_1 + w_2 \in W) \;\blacksquare\; L\big(S(w_1+w_2)\big) = w_1 + w_2$

(3.5.3) $L\big(S(w_1)+S(w_2)\big) = w_1 + w_2 = L\big(S(w_1+w_2)\big) \;\blacksquare\; L\big(S(w_1)+S(w_2)\big) = L\big(S(w_1+w_2)\big)$

(3.5.4) $(Injective[L,V,W]) \wedge \Big(L\big(S(w_1)+S(w_2)\big) = L\big(S(w_1+w_2)\big)\Big) \;\blacksquare\; S(w_1)+S(w_2) = S(w_1+w_2)$

(3.6) $(w_1, w_2 \implies W) \implies \big(S(w_1+w_2) = S(w_1)+S(w_2)\big) \;\blacksquare\; \forall_{w_1,w_2\in W}\big(S(w_1+w_2) = S(w_1)+S(w_2)\big)$

(3.7) $\big((r \in \mathbb{R}) \wedge (w \in W)\big) \implies \ldots$

(3.7.1) $(LinTrans[L,V,+_v,*_v,W,+_w,*_w]) \wedge \Big(\forall_{w\in W}\Big(L\big(S(w)\big) = w\Big)\Big) \;\blacksquare\; L\big(r * S(w)\big) = r * L\big(S(w)\big) = r * w$

(3.7.2) $\Big(\forall_{w\in W}\Big(L\big(S(w)\big) = w\Big)\Big) \wedge (r * w \in W) \;\blacksquare\; L\big(S(r*w)\big) = r * w$

(3.7.3) $L\big(r * S(w)\big) = r * w = L\big(S(r*w)\big) \;\blacksquare\; L\big(r * S(w)\big) = L\big(S(r*w)\big)$

(3.7.4) $(Injective[L,V,W]) \wedge \Big(L\big(r * S(w)\big) = L\big(S(r*w)\big)\Big) \;\blacksquare\; r * S(w) = S(r*w)$

(3.8) $\big((r \in \mathbb{R}) \wedge (w \in W)\big) \implies \big(r * S(w) = S(r*w)\big) \;\blacksquare\; \forall_{r\in\mathbb{R}}\forall_{w\in W}(S(r*w) = r * S(w)$

(3.9) $(Function[S,W,V]) \wedge \Big(\forall_{w_1,w_2\in W}\big(S(w_1+w_2) = S(w_1)+S(w_2)\big)\Big) \wedge \Big(\forall_{r\in\mathbb{R}}\forall_{w\in W}\big(S(r*w) = r * S(w)\big)\Big)$

(3.10) $LinTrans[S,W,+_w,*_w,V,+_v,*_v]$

(3.11) $\forall_{v\in V}\Big(\Big(S\big(L(v)\big) = v\Big)\Big) \;\blacksquare\; S \circ L = 1_v$

(3.12) $\forall_{w\in W}\Big(L\big(S(w)\big) = w\Big) \;\blacksquare\; L \circ S = 1_w$

(3.13) $(LinTrans[S,W,+_w,*_w,V,+_v,*_v]) \wedge (S \circ L = 1_v) \wedge (L \circ S = 1_w) \;\blacksquare\; LTInv[S,L,V,+_v,*_v,W,+_w,*_w]$

(3.14) $\exists_{L^{-1}}(LTInv[L^{-1},L,V,+_v,*_v,W,+_w,*_w]) \;\blacksquare\; LTInvertible[L,V,+_v,*_v,W,+_w,*_w]$

(4) $\big((Injective[L,V,W]) \wedge (Surjective[L,V,W])\big) \implies (LTInvertible[L,V,+_v,*_v,W,+_w,*_w])$

(5) $(LTInvertible[L, V, +_v, *_v, W, +_w, *_w]) \iff \big((Injective[L, V, W]) \wedge (Surjective[L, V, W])\big)$

TODO: some corollary of InjectiveSurjectiveEqualDim + SurjectiveInjectiveEqualDim + InvertibleBijectiveEquiv

$Isomorphism[L, V, +_v, *_v, W, +_w, *_w] := LTInvertible[L, V, +_v, *_v, W, +_w, *_w]$
$Isomorphic[V, +_v, *_v, W, +_w, *_w] := \exists_L(Isomorphism[L, V, +_v, *_v, W, +_w, *_w])$

3.9 Matrix of a Linear Transform

$CoordVec[[\alpha]_S, \alpha, S, V, +, *] := (Basis[S, V, +, *]) \wedge (S * [\alpha]_S = \alpha \in V)$

$$LTMatrix := \forall_{L,V,W}\left(\begin{array}{l}\big((LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (Basis[A, V, +_v, *_v]) \wedge (Basis[B, W, +_w, *_w])\big) \qquad \Longrightarrow \\ \Big(\forall_{v \in V}\big(CoordVec[[L(v)]_B, L(v), B, W, +_w, *_w] = \langle [L(a_i)]_B | a_i \in A\rangle * CoordVec[[v]_A, v, A, V, +_v, *_v]\big)\Big)\end{array}\right)$$

(1) $Basis[A, V, +_v, *_v] \ \blacksquare\ \exists_{K \in \mathbb{R}^n}\big(v = \sum_{i=1}^n (k_i * a_i)\big) \ \blacksquare\ K^T = CoordVec[[v]_A, , v, A, V, +, *]$

(2) $[L(v)]_B = [L\big(\sum_{i=1}^n (k_i * a_i)\big)]_B = [\sum_{i=1}^n \big(L(k_i * a_i)\big)]_B = \sum_{i=1}^n \big([L(k_i * a_i)]_B\big) = \sum_{i=1}^n \big([k_i * L(a_i)]_B\big) = \sum_{i=1}^n \big(k_i * [L(a_i)]_B\big) = \ \ldots$

(3) $\ldots \langle [L(a)]_B | a \in A\rangle * K^T = \langle [L(a)]_B | a \in A\rangle * [v]_A \ \blacksquare\ [L(v)]_B = \langle [L(a)]_B | a \in A\rangle * [v]_A$

Note: Shorthand is to RREF the augmented matrix [Columns of B | Columns of A] into [I | M], thus M is the transition matrix

$$TransitionMatrix := \forall_{L,V}\left(\begin{array}{l}\big((Basis[A, V, +, *]) \wedge (Basis[B, V, +, *])\big) \qquad \Longrightarrow \\ \big(\forall_{v \in V}(CoordVec[[v]_B, v, B, W, +_w, *_w] = \langle [a]_B | a \in A\rangle * CoordVec[[v]_A, v, A, V, +_v, *_v])\big)\end{array}\right)$$

(1) $(LTMatrix) \wedge (LinTrans[I, V, +, *, V, +, *]) \ \blacksquare\ [I(v)]_B = \langle [I(a)]_B | a \in A\rangle * [v]_A \ \blacksquare\ [v]_B = \langle [a]_B | a \in A\rangle * [v]_A$

$$LTOverTransition := \Big(\big([L(a)]_T = A * [a]_S\big) \wedge (P * [a]_{S'} = [a]_S) \wedge \big(Q * [L(a)]_{T'} = [L(a)]_T\big)\Big) \implies \Big([L(a)]_{T'} = (Q^{-1} * A * P) * [a]_{S'}\Big)$$

(1) $[L(a)]_{T'} = Q^{-1} * [L(a)]_T = Q^{-1} * A * [a]_S = Q^{-1} * A * P * [a]_{S'} \ \blacksquare\ [L(a)]_{T'} = (Q^{-1} * A * P) * [a]_{S'}$

$$LOOverTransition := \Big(\big([L(a)]_S = A * [a]_S\big) \wedge (P * [a]_{S'} = [a]_S)\Big) \implies \Big([L(a)]_{S'} = (P^{-1} * A * P) * [a]_{S'}\Big)$$

(1) $P * [a]_{S'} = [a]_S \ \blacksquare\ P * [L(a)]_{S'} = [L(a)]_S$

(2) $LTOverTransition \ \blacksquare\ [L(a)]_{S'} = P^{-1} * [L(a)]_S = P^{-1} * A * [a]_S = P^{-1} * A * P * [a]_{S'} \ \blacksquare\ [L(a)]_{S'} = (P^{-1} * A * P) * [a]_{S'}$

$RankNullityRelation := (Rank[A] \equiv Dim[rng_L]) \wedge (Nullity[A] \equiv Dim[ker_L]) \wedge (RankNullity \equiv RankNullityLT)$

(1) TODO

$SimMatrix[A, B] := \exists_P(B = P * A * P^{-1})$

$SimMatrixEquiv := (SimMatrix[A, B]) \iff \Big(\big([L(a)]_T = A * [a]_S\big) \wedge \big([L(a)]_{T'} = B * [a]_{S'}\big)\Big)$???