Contents

Chapter 1

Real Analysis

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

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

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

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

(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) $\forall_E((\emptyset \neq E \subset S \wedge BoundedAbove[E, S, <]) \implies \exists_{\alpha \in S}(LUB[\alpha, E, S, <]))$ — 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) $b_1 := choice(\{{b_1}' \in B : \exists_{b_0' \in B}({b_0}' < {b_1}')\}) \blacksquare \neg LowerBound[b_1, B, S, <]$ — 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) $\forall_{x \in B}(x \in S \wedge \forall_{y \in L}(y_0 \leq x)) \blacksquare \forall_{x \in B}(UpperBound[x, L, S, <])$ — 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) $\exists_{\alpha' \in S}(LUB[\alpha', L, S, <]) \blacksquare \alpha := choice(\{\alpha' \in S : (LUB[\alpha', L, S, <])\})$ — 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) $(|B| = 1 \implies \exists_{\epsilon_0 \in S}(GLB[\epsilon_0, B, S, <])) \wedge (|B| \neq 1 \implies \exists_{\epsilon_1 \in S}(GLB[\epsilon_1, B, S, <]))$ — 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) $\forall_B((\emptyset \neq B \subset S \wedge BoundedBelow[B, S, <]) \implies \exists_{\epsilon \in S}(GLB[\epsilon, B, S, <]))$

(1.4) $GLBProperty[S, <]$

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

(1.12)

$$Field[F, +, *] := \exists_{0,1 \in F} \forall_{x,y,z \in F} \begin{pmatrix} x + y \in F & \wedge & x * y \in F & \wedge \\ x + y = y + x & \wedge & x * y = y * x & \wedge \\ (x + y) + z = x + (y_0 + z) & \wedge & (x * y) * z = x * (y_0 * z) & \wedge \\ \mathbb{1} \neq \mathbb{0} & \wedge & x * (y_0 + z) = (x * y) + (x * z) & \wedge \\ \mathbb{0} + x = x & \wedge & \mathbb{1} * x = x & \wedge \\ \exists_{-x \in F}(x + (-x) = \mathbb{0}) \wedge (x \neq \mathbb{0} \implies \exists_{1/x \in F}(x * (1/x) = \mathbb{1})) & & & \end{pmatrix}$$

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

(1.14)

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

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

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

(2) $x = -(-x)$ — from: $AdditiveInverseUniqueness$

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

(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: *Field*

(2) $\mathbb{0} * x = \mathbb{0}$ — from: *AdditiveIdentityUniqueness*

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

(1) $(x \neq \mathbb{0} \wedge y \neq \mathbb{0}) \implies \ldots$
- (1.1) $(x * y = 0) \implies \ldots$
  - (1.1.1) $\mathbb{1} = \mathbb{1} * \mathbb{1} = (x * (1/x)) * (y * (1/y)) = (x * y) * ((1/x) * (1/y)) = \mathbb{0} * ((1/x) * (1/y)) = \mathbb{0}$ — from: *Field*, *Domination*, 1, 1.1
  - (1.1.2) $\mathbb{1} = \mathbb{0} \wedge \mathbb{1} \neq \mathbb{0}$ ▮ $\bot$ — from: *Field*
- (1.2) $(x * y = 0) \implies \bot$ ▮ $x * y \neq 0$

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

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

(1) $x * y + (-x) * y = (x + -x) * y = \mathbb{0} * y = \mathbb{0}$ ▮ $x * y + (-x) * y = \mathbb{0}$ — from: *Field*, *Domination* wts: 2

(2) $(-x) * y = -(x * y)$ — from: *AdditiveInverseUniqueness*

(3) $x * y + x * (-y) = x * (y_0 + -y) = x * \mathbb{0} = \mathbb{0}$ ▮ $x * y + x * (-y) = \mathbb{0}$ — from: *Field*, *Domination* wts: 4

(4) $x * (-y) = -(x * y)$ — from: *AdditiveInverseUniqueness*

(5) $(-x) * y = -(x * y) = x * (-y)$ — from: 2, 4

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

(1) $(-x) * (-y) = -(x * (-y)) = -(-(x * y)) = x * y$ — from: *NegationCommutativity*, *DoubleNegative*

(1.17)
$$OrderedField[F, +, *, <] := \begin{pmatrix} Field[F, +, *] \quad \wedge \quad Order[<, F] \quad \wedge \\ \forall_{x,y,z \in F}(y_0 < z \implies x + y < x + z) \wedge \\ \forall_{x,y \in F}((x > \mathbb{0} \wedge y > \mathbb{0}) \implies x * y > \mathbb{0}) \end{pmatrix}$$

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

(1.18)
$NegationOnOrder := x > \mathbb{0} \iff -x < \mathbb{0}$

(1) $x > \mathbb{0} \implies \ldots$
- (1.1) $\mathbb{0} = (-x) + x > (-x) + \mathbb{0} = -x$ ▮ $\mathbb{0} > -x$ ▮ $-x < \mathbb{0}$ — from: *OrderedField*

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

(3) $-x < \mathbb{0} \implies \ldots$
- (3.1) $\mathbb{0} = x + (-x) < x + \mathbb{0} = x$ ▮ $\mathbb{0} < x$ ▮ $x > \mathbb{0}$ — from: *OrderedField*

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

(5) $x > \mathbb{0} \implies -x < \mathbb{0} \wedge -x < \mathbb{0} \implies x > \mathbb{0}$ ▮ $x > \mathbb{0} \iff -x < \mathbb{0}$ — from: 2, 4

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

(1) $(x > \mathbb{0} \wedge y < z) \implies \ldots$
- (1.1) $(-y) + z > (-y) + y = \mathbb{0}$ ▮ $z + (-y) = \mathbb{0}$ — from: *OrderedField*
- (1.2) $x * (z + (-y)) > \mathbb{0}$ ▮ $x * z + x * (-y) > \mathbb{0}$ — from: *OrderedField*
- (1.3) $x * z = \mathbb{0} + x * z = (x * y + -(x * y)) + x * z = (x * y + x * (-y)) + x * z = \ldots$ — from: *Field*, *NegationCommutativity*
- (1.4) $x * y + (x * z + x * (-y)) > x * y + \mathbb{0} = x * y$ — 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) $1/x < \mathbb{0} \implies x * (1/x) < 0 \wedge x * (1/x) > 0 \implies \bot \;\blacksquare\; 1/x > \mathbb{0}$ — from: *NegativeFactorFlipsOrder*, 1

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

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

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

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

(1.19)
OrderedFieldQ $:= \mathit{OrderedField}[\mathbb{Q}, +, *, <]$ —

Subfield$[K, F, +, *] := \mathit{Field}[F, +, *] \wedge K \subset F \wedge \mathit{Field}[K, +, *]$
OrderedSubfield$[K, F, +, *, <] := \mathit{OrderedField}[F, +, *, <] \wedge K \subset F \wedge \mathit{OrderedField}[K, +, *, <]$
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$[\alpha] := \forall_{p \in \alpha} \exists_{r \in \alpha} (p < r)$
$\mathbb{R} := \{\alpha \in \mathbb{Q} : \mathit{CutI}[\alpha] \wedge \mathit{CutII}[\alpha] \wedge \mathit{CutIII}[\alpha]\}$

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) $(q = p) \implies (p \in \alpha \wedge p \notin \alpha) \implies \bot \;\blacksquare\; q \neq p$ — 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) $(\alpha \in \mathbb{R} \wedge p \in \alpha \wedge q \in \mathbb{Q} \wedge q \notin \alpha) \implies p < q$

$CutCorollary11 := (\alpha \in \mathbb{R} \wedge r, s \in \mathbb{Q} \wedge r < s \wedge r \notin \alpha) \implies s \notin \alpha$

(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: $Cut11$, 1

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

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

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

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

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

(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) $\exists_{p'}(p' \in \alpha \wedge p' \notin \beta)$ ▮ $p := choice(\{p' : p' \in \alpha \wedge p' \notin \beta\})$

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

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

(1.1.3.2) $q < p$ from: $CutCorollary1$

(1.1.3.3) $q \in \alpha$ from: $Cut11$

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

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

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

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

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

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

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

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

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

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

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

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

$OrderOf R := Order[<_{\mathbb{R}}, \mathbb{R}]$ from: $OrderTrichotomyR, OrderTransitivityR$
wts:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$+_{\mathbb{R}}[\alpha, \beta] := \alpha, \beta \in \mathbb{R} \wedge (\alpha +_{\mathbb{R}} \beta) = \{r + s : r \in \alpha \wedge s \in \beta\}$
$0_{\mathbb{R}} := \{x \in \mathbb{Q} : x < 0\}$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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) $-t_0 - (r_1/2) = -(p + (r_1/2)) - (r_1/2) = -p - r_1$

(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) $\exists_{n\in\mathbb{Z}}(nw_0 \in \alpha \wedge (n+1)w_0 \notin \alpha) \ \blacksquare\ n_0 := choice(\{n \in \mathbb{Z} : nw_0 \in \alpha \wedge (n+1)w_0 \notin \alpha\})$ 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) $\beta \in \mathbb{R} \wedge \alpha +_{\mathbb{R}} \beta = 0_{\mathbb{R}} \ \blacksquare\ \exists_{-\alpha\in\mathbb{R}}(\alpha +_{\mathbb{R}} (-\alpha) = 0_{\mathbb{R}})$

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

$*_{\mathbb{R}}[\alpha, \beta] :=$ —

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1.20)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1.21)

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

(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) $b/a > 1 \ \blacksquare \ \sum_{i=1}^{n}(b^{n-i}a^{i-1}) \leq \sum_{i=1}^{n}(b^{n-i}a^{i-1}(b/a)^{i-1}) = \sum_{i=1}^{n}(b^{n-1}) = nb^{n-1} \ \blacksquare \ \sum_{i=1}^{n}(b^{n-i}a^{i-1}) \leq \sum_{i=1}^{n}(b^{n-1}) = nb^{n-1}$

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

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

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

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

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

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

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

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

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

(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) $(t \in E) \wedge (t \in E \iff (t \in \mathbb{R} \wedge t > 0 \wedge t^n < x))$ ▌ $t^n < x$

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

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

(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) $(0 < x - {y_0}^n) \wedge (0 < n(y_0 + 1)^{n-1})$ ▌ $0 < \frac{x - {y_0}^n}{n(y_0+1)^{n-1}} = k_0$ ▌ $0 < k_0$

(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) $QDenseInR \wedge (0, min(1, k_0) \in \mathbb{R}) \wedge (0 < min(1, k_0))$ ▌ $\exists_{h \in \mathbb{Q}}(0 < h < min(1, k_0)) \ \ldots$

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

(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) $((y_0 + h_0)^n - {y_0}^n < h_0 n (y_0 + h_0)^{n-1}) \wedge (h_0 n (y_0 + h_0)^{n-1} < h_0 n (y_0 + 1)^{n-1})$ ▌ $(y_0 + h_0)^n - {y_0}^n < h_0 n (y_0 + 1)^{n-1}$

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

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

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

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

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

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

(1.22) ${y_0}^n < x \implies \bot$ ▌ ${y_0}^n \geq x$

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

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

(1.23.2) $(0 < x) \wedge (0 < n \in \mathbb{Z})$ ▌ ${y_0}^n - x < {y_0}^n \leq n {y_0}^n$ ▌ ${y_0}^n - x < n {y_0}^n$

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

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

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

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

(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) $t \geq y_0 - k_1 \implies \ldots$

(1.23.8.1) $t \geq y_0 - k_1 \ \blacksquare\ {t^n} \geq (y_0 - k_1)^n \ \blacksquare\ -t^n \leq -(y_0 - k_1)^n \ \blacksquare\ {y_0}^n - t^n \leq {y_0}^n - (y_0 - k_1)^n$

(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) $({y_0}^n - t^n \leq {y_0}^n - (y_0 - k_1)^n) \wedge ({y_0}^n - (y_0 - k_1)^n < k_1 n {y_0}^{n-1}) \ \blacksquare\ {y_0}^n - t^n < k_1 n {y_0}^{n-1}$

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

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

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

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

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

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

(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) $y_1 \neq y_2 \implies \ldots$

(1.29.1) $(OrderTrichotomy[\mathbb{R}, <]) \wedge (y_1 \neq y_2) \ \blacksquare\ (y_1 < y_2) \veebar (y_2 < y_1) \ \ldots$

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

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

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

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

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

$$ExtendedRealSystem[\bar{\mathbb{R}}, +, *, <] := \begin{pmatrix} \bar{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\} & \wedge & -\infty < x < \infty & \wedge \\ x + \infty = +\infty \ \wedge \ x - \infty = -\infty \ \wedge \ \frac{x}{+\infty} = \frac{x}{-\infty} = 0 \wedge & & & \\ (x > 0) \implies (x * (+\infty) = +\infty \wedge x * (-\infty) = -\infty) \wedge & & & \\ (x < 0) \implies (x * (+\infty) = -\infty \wedge x * (-\infty) = +\infty) & & & \end{pmatrix}$$

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

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

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

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

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

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

(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) $0 \leq z * \overline{z} \in \mathbb{R}$

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

(1) 123123

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

Chapter 2

Abstract Algebra

2.1 Functions

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

$FuncComp := (Comp[g \circ f, f, g, X, Y, Z]) \implies (Func[g \circ f, X, Z])$

(1) TODO

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

(1) TODO

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

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

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

(1) TODO

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

(1) TODO

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

(1) TODO

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

(1) TODO

2.2 Divisibility, Equivalence Relations, Paritions

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

(1) TODO

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

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

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

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

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

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

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

(1) TODO

2.3 Groups

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

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

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

(1) $(a*b = a*c) \implies \ldots$
  (1.1) $a \in G$ ▮ $\exists_{a^{-1}\in G}(a*a^{-1} = e = a^{-1}*a)$
  (1.2) $Function[*,G,G]$ ▮ $a^{-1}*a*b = a^{-1}*a*c$
  (1.3) $(\forall_{a,b,c\in G}((a*b)*c = a*(b*c))) \wedge (\forall_{a\in G}\exists_{a^{-1}\in G}(a*a^{-1} = e = a^{-1}*a))$ ▮ $b = c$
(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) $((a*b = a*c) \implies (b = c)) \wedge ((a*c = b*c) \implies (a = b))$

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

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

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

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

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

(1) $(a*b)*(a*b)^{-1} = e$
(2) $(a*b)*(b^{-1}*a^{-1}) = (a*(b*b^{-1})*a^{-1}) = e$
(3) $InvUniq$ ▮ $(a*b)^{-1} = b^{-1}*a^{-1}$

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

2.4 Subgroups

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

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

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

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

- (2.1) $Group[G, *]$ ▌ $(a, b, c \in H) \implies (a, b, c \in G) \implies ((a * b) * c = a * (b * c))$ ▌ $\forall_{a,b,c \in H}((a * b) * c = a * (b * c))$
- (2.2) $\emptyset \neq H$ ▌ $\exists_h(h \in H)$
- (2.3) $h \in H$ ▌ $\exists_{h^{-1} \in H}(h * h^{-1} = e = h^{-1} * h)$
- (2.4) $Function[*, H, H]$ ▌ $e = h * h^{-1} \in H$ ▌ $e \in H$ ▌ $\exists_{e \in H}\forall_{a \in H}(a * e = a = e * a)$
- (2.5) $(Function[*, H, H]) \wedge (\forall_{a,b,c \in H}((a * b) * c = a * (b * c))) \wedge (\exists_{e \in H}\forall_{a \in H}(a * e = a = e * a) \wedge (\forall_{a \in H}\exists_{a^{-1} \in H}(a * a^{-1} = e = a^{-1} * a))$
- (2.6) $Group[H, *]$
- (2.7) $(Group[G, *]) \wedge (H \subseteq G) \wedge (Group[H, *])$ ▌ $Subgroup[H, G, *]$

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

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

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

(1) TODO

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

(1) $Group[G, *]$

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

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

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

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

- (5.1) $a, b \in H_1$ ▌ $a * b \in H_1$
- (5.2) $a, b \in H_2$ ▌ $a * b \in H_2$
- (5.3) $a * b \in H_1 \cap H_2$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5 Special Groups

2.5.1 Cyclic Group

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

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

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

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

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

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

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

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

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

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

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

(4) $(b \in H) \implies (b \in < g^m >)$ ▌ $H \subseteq < g^m >$

(5) $(b \in < g^m >) \implies \ldots$

(5.1) $\exists_{k \in \mathbb{Z}}(b = g^{mk})$

(5.2) $g^m \in H$ ▌ $b = g^{mk} \in H$ ▌ $b \in H$

(6) $(b \in < g^m >) \implies (b \in H)$ ▌ $< g^m > \subseteq H$

(7) $(H \subseteq < g^m >) \wedge (< g^m > \subseteq H)$ ▌ $H = < g^m >$ ▌ $Generator[g^m, H, *]$ ▌ $\exists_{h \in G}(Generator[h, G, *])$ ▌ $CyclicGroup[H, *]$

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

(1) $(s \equiv t (mod\ n)) \iff (Divides[n, s - t]) \iff (\exists_{k \in \mathbb{N}}(s - t = kn)) \iff \ldots$

(2) $\ldots (\exists_{k \in \mathbb{N}}(s = kn + t)) \iff (g^s = g^{kn+t} = g^{kn} * g^t = e^k * g^t = g^t) \iff (g^s = g^t)$

$ExpModOrderCorollary := \forall_{G,g,n,s,t}(((Group[G, *]) \wedge (OrderEl[n, g, G, *])) \implies ((g^s = e) \iff (Divides[n, s])))$

(1) $ExpModOrder$ ▌ $(g^s = e) \iff (g^s = g^0) \iff (s \equiv 0 (mod\ n)) \iff (Divides[n, s - 0]) \iff (Divides[n, s])$

2.5.2 Symmetric and Alternating Groups

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

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

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

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

2.5.3 Dihedral Group

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

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

2.6 Lagrange's Theorem

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

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

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

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

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

(1.1) $(Subgroup[H, G, *]) \implies (e \in H) \implies (a * a^{-1} \in H) \implies (a \sim a)$

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

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

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

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

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

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

$CosetSet[G : H, H, G, *] := (Subgroup[H, G, *]) \land (G : H = \{gH | g \in G\})$
$IndexSubgroup[|G : H|, H, G, *] := (CosetSet[G : H, H, G, *]) \land (|G : H| = |G : H|) \land (|G| = (|H|)(|G : H|))$

$LagrangeTheorem := \forall_{G,H}(((Subgroup[H, G, *]) \land (o(G), o(H) \in \mathbb{N})) \implies (o(G) = o(H)|G : H|) \land (Divides[o(H), o(G)])$

(1) $(CosetInduceEqRel) \land (EqRelInducesPartition) \land (CosetCardinality) \blacksquare (o(G) = o(H)|G : H|) \land (Divides[o(H), o(G)])$

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

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

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

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

(2) CyclicSubgroup of a non-identity element is G ▌ Non-identity elements generates G

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

(1) $(LagrangeTheorem) \land (SubgroupIntersection) \land (RelPrime(o(H), o(K)))$ ▌ $H \cap K = \{e\}$

2.7 Homomorphisms

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

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

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

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

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

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

$ExpMapsExp := (Homomorphism[\phi, G, *, H, \diamond]) \implies (\forall_{n \in \mathbb{N}^+}(\phi(g^n) = \phi(g)^n))$

(1) $\phi(g^1) = \phi(g) = \phi(g)^1$ ▌ $\phi(g^1) = \phi(g)^1$

(2) $(\forall_{k \in \mathbb{N}^+}(\phi(g^k) = \phi(g)^k)) \implies \ldots$

(2.1) $\phi(g^{k+1}) = \phi(g^k * g) = \phi(g)^k \diamond \phi(g) = \phi(g)^{k+1}$ ▌ $\phi(g^{k+1}) = \phi(g)^{k+1}$

(3) $(\forall_{k \in \mathbb{N}^+}(\phi(g^k) = \phi(g)^k)) \implies (\phi(g^{k+1}) = \phi(g)^{k+1})$

(4) $(\phi(g^1) = \phi(g)^1) \land ((\forall_{k \in \mathbb{N}^+}(\phi(g^k) = \phi(g)^k)) \implies (\phi(g^{k+1}) = \phi(g)^{k+1}))$ ▌ $\forall_{n \in \mathbb{N}^+}(\phi(g^n) = \phi(g)^n))$

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

(1) $OrderOrderElProp$ ▌ $g^n = e_G$

(2) $(IdMapsId) \land (ExpMapsExp)$ ▌ $e_G = \phi(g^n) = \phi(g)^n = e_H$

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

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

(1) $FuncComp$ ▌ $Func[\theta \circ \phi, G, K]$

(2) $(g_1, g_2 \in G) \implies \ldots$

(2.1) $(Homomorphism[\phi, G, *, H, \diamond]) \land (Homomorphism[\theta, H, \diamond, K, \square])$ ▌ $\theta \circ \phi(g_1 * g_2) = \theta(\phi(g_1 * g_2)) = \ldots$

(2.2) $\ldots \theta(\phi(g_1) \diamond \phi(g_2)) = \theta(\phi(g_1)) \square \theta(\phi(g_2)) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2)$ ▌ $\theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2)$

(3) $(g_1, g_2 \in G) \implies (\theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2))$ ▌ $\forall_{g_1, g_2 \in G}(\theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2))$

(4) $(Func[\theta \circ \phi, G, K]) \land (\forall_{g_1, g_2 \in G}(\theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2)))$ ▌ $Homomorphism[\theta \circ \phi, G, *, K, \square]$

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

(1) $Isomorphism[\phi, G, *, H, \diamond]$ ▌ $(Homomorphism[\phi, G, *, H, \diamond]) \land (Bij[\phi, G, H])$

(2) $BijEquiv$ ▌ $\exists_{\phi^{-1}}(Inv[\phi^{-1}, \phi, G, H])$

(3) TODO continue

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

(1) $\exists_{g,h}((Generator[g,G,*]) \wedge (Generator[h,H,\diamond]))$

(2) TODO $\phi(g^n) = h^n$

2.8 Kernel and Image Homomorphisms

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

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

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

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

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

  (3.1) $(\phi(a) = e_H) \wedge (\phi(b) = e_H) \blacksquare \phi(a * b) = \phi(a) \diamond \phi(b) = e_H \diamond e_H = e_H \blacksquare a * b \in ker_\phi$

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

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

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

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

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

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

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

(1) $(IdMapsId) \wedge (e_G \in G) \blacksquare \phi(e_G) = e_H \in H \blacksquare e_H \in im_\phi \blacksquare \emptyset \neq im_\phi$

(2) $im_\phi \subseteq H \blacksquare \emptyset \neq im_\phi \subseteq H$

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

  (3.1) $(\exists_{g_a \in G}(a = \phi(g_a))) \wedge (\exists_{g_b \in G}(b = \phi(g_b)))$

  (3.2) $(g_a * g_b \in G) \wedge (\phi(g_a * g_b) = \phi(g_a) * \phi(g_b) = a * b)$

  (3.3) $\exists_{g \in G}(a * b = \phi(g)) \blacksquare a * b \in im_\phi$

(4) $(a, b \in im_\phi) \implies (a * b \in im_\phi) \blacksquare \forall_{a,b \in im_\phi}(a * b \in im_\phi)$

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

  (5.1) $\exists_{g_a \in G}(a = \phi(g_a))$

  (5.2) $({g_a}^{-1} \in G) \wedge (InvMapsInv) \blacksquare \phi({g_a}^{-1}) = \phi(g_a)^{-1} = a^{-1}$

  (5.3) $\exists_{g \in G}(a^{-1} = \phi(g)) \blacksquare a^{-1} \in im_\phi$

(6) $(a \in im_\phi) \implies (a^{-1} \in im_\phi) \blacksquare \forall_{a \in im_\phi}(a^{-1} \in im_\phi)$

(7) $(SubgroupEquiv) \wedge (\emptyset \neq im_\phi \subseteq H) \wedge (\forall_{a,b \in im_\phi}(a * b \in im_\phi)) \wedge (\forall_{a \in im_\phi}(a^{-1} \in im_\phi)) \blacksquare Subgroup[im_\phi, H, \diamond]$

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

(1) $CyclicGroup[G, *] \blacksquare \exists_{g \in G}(CyclicSubgroup[G, g, G, *]) \blacksquare \exists_{g_0 \in G}(G =< g_0 >= \{{g_0}^n | n \in \mathbb{Z}\})$

(2) $ExpMapsExp \blacksquare h \in im_\phi \iff \exists_{g \in G}(h = \phi(g)) \iff \exists_{n \in \mathbb{Z}}(h = \phi({g_0}^n)) \iff \exists_{n \in \mathbb{Z}}(h = \phi(g_0)^n) \blacksquare Generator[\phi(g_0), im_\phi, \diamond]$

(3) $\exists_{h \in im_\phi}(Generator[h, im_\phi, \diamond]) \blacksquare CyclicGroup[im_\phi, \diamond]$

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

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

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

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

(1.2.1) $(g \in ker_\phi) \wedge (IdMapsId) \blacksquare \phi(g) = e_H = \phi(e_G)$

(1.2.2) $(Injective[\phi, G, H]) \wedge (\phi(g) = \phi(e_G)) \blacksquare g = e_G \blacksquare g \in \{e_G\}$

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

(1.4) $(\{e_G\} \subseteq ker_\phi) \wedge (ker_\phi \subseteq \{e_G\}) \blacksquare ker_\phi = \{e_G\}$

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

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

(3.1) $((g_1, g_2 \in G) \wedge (\phi(g_1) = \phi(g_2))) \implies \ldots$

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

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

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

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

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

$KerCountsMapSameEl := ((Homomorphism[\phi, G, *, H, \diamond]) \wedge (g \in G)) \implies ((ker_\phi)g = \{x \in G | \phi(x) = \phi(g)\})$

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

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

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

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

(5) $((ker_\phi)g \subseteq \{x \in G | \phi(x) = \phi(g)\}) \wedge (\{x \in G | \phi(x) = \phi(g)\} \subseteq (ker_\phi)g) \blacksquare (ker_\phi)g = \{x \in G | \phi(x) = \phi(g)\}$

$KerImPartitionsG := (Homomorphism[\phi, G, *, H, \diamond]) \implies (o(G) = o(ker_\phi)o(im_\phi))$

(1) im_ϕ forms equivalence classes of G that maps to the same elements under ϕ

(2) $(KerCountsMapSameEl) \wedge (CosetCardinality)$ counts the number of same element mappings / multiplicity for each pre-image class

(3) $o(G) = o(ker_\phi)o(im_\phi)$

(4) TODO: formalize

$ImageDividesGH := (Homomorphism[\phi, G, *, H, \diamond]) \implies ((Divides[o(im_\phi), o(G)]) \wedge (Divides[o(im_\phi), o(H)]))$

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

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

2.9 Conjugacy

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

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

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

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

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

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

$ConjugacyClassEquiv := (ConjugacyClass[C_g, g, G, *]) \iff (\forall_{x \in G}((x \in C_g) \iff (\exists_{c \in G}(x = c^{-1}gc))))$

(1) TODO: by definition

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

(1) $(C_g = \{g\}) \implies \ldots$

(1.1) $(x \in G) \implies \ldots$

(1.1.1) $(ConjugacyClass[C_g, g, G, *]) \land (ConjugacyClassEquiv) \land (x \in G)$ ▮ $x^{-1}gx \in C_g$

(1.1.2) $(C_g = \{g\}) \land (x^{-1}gx \in C_g)$ ▮ $x^{-1}gx = g$ ▮ $gx = xg$

(1.2) $(x \in G) \implies (gx = xg)$ ▮ $\forall_{x \in G}(gx = xg)$ ▮ $g \in Z(G)$

(2) $(C_g = \{g\}) \implies (g \in Z(G))$

(3) $(g \in Z(G)) \implies \ldots$

(3.1) $(g \in Z(G)) \land (Group[G, *])$ ▮ $(\forall_{c \in G}(gc = cg)) \land (\exists_e(e \in G))$

(3.2) $(x \in G) \implies \ldots$

(3.2.1) $(\forall_{c \in G}(gc = cg)) \land (\exists_e(e \in G))$ ▮ $(\exists_{c \in G}(x = c^{-1}gc)) \iff (\exists_{c \in G}(x = c^{-1}gc = c^{-1}cg = g)) \iff (x = g) \iff (x \in \{g\})$

(3.3) $(x \in G) \implies ((\exists_{c \in G}(x = c^{-1}gc)) \iff (x \in \{g\}))$ ▮ $\forall_{x \in G}((x \in \{g\}) \iff (\exists_{c \in G}(x = c^{-1}gc)))$

(3.4) $(ConjugacyClassEquiv) \land (\forall_{x \in G}((x \in \{g\}) \iff (\exists_{c \in G}(x = c^{-1}gc))))$ ▮ $C_g = \{g\}$

(4) $(g \in Z(G)) \implies (C_g = \{g\})$

(5) $(C_g = \{g\}) \iff (g \in Z(G))$

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

(1) $ConjugacyCenter$ ▮ $(\forall_{g \in G}(C_g = \{g\})) \iff (\forall_{g \in G}(g \in Z(g))) \iff (AbelianGroup[G, *])$

$ConjugateExp := \forall_{n \in \mathbb{N}^+}((x^{-1}gx)^n = x^{-1}g^nx)$

(1) $(n = 1) \implies \ldots$

(1.1) $(x^{-1}gx)^n = (x^{-1}gx)^1 = x^{-1}g^1x = x^{-1}g^nx$ ▮ $(x^{-1}gx)^n = x^{-1}g^nx$

(2) $(n = 1) \implies ((x^{-1}gx)^n = x^{-1}g^nx)$

(3) $((n > 1) \land (\forall_{m \in \mathbb{N}^+}((m \leq n) \implies ((x^{-1}gx)^m = x^{-1}g^mx)))) \implies \ldots$

(3.1) $(x^{-1}gx)^{n+1} = (x^{-1}gx)^n * (x^{-1}gx) = (x^{-1}g^nx) * (x^{-1}gx) = x^{-1}g^{n+1}x$ ▮ $(x^{-1}gx)^{n+1} = x^{-1}g^{n+1}x$

(4) $((n > 1) \land (\forall_{m \in \mathbb{N}^+}((m \leq n) \implies ((x^{-1}gx)^m = x^{-1}g^mx)))) \implies ((x^{-1}gx)^{n+1} = x^{-1}g^{n+1}x)$

(5) $\forall_{n \in \mathbb{N}^+}((x^{-1}gx)^n = x^{-1}g^nx)$

$ConjugateOrder := ((g_1, g_2 \in G) \land (g_1 \sim^* g_2)) \implies (o(g_1) = o(g_2))$

(1) $\exists_{c \in G}(g_2 = c^{-1}g_1c)$

(2) $ConjugateExp$ ▮ $e = {g_2}^{o(g_2)} = (c^{-1}g_1c)^{o(g_2)} = c^{-1}{g_1}^{o(g_2)}c$ ▮ $e = c^{-1}{g_1}^{o(g_2)}c$ ▮ ${g_1}^{o(g_2)} = e$

(3) $ExpModOrderCorollary$ ▮ $Divides[o(g_2), o(g_1)]$

(4) $ConjugateExp$ ▮ $e = {g_1}^{o(g_1)} = (cg_2c^{-1})^{o(g_1)} = c{g_2}^{o(g_1)}c^{-1}$ ▮ $e = c{g_2}^{o(g_1)}c^{-1}$ ▮ ${g_2}^{o(g_1)} = e$

(5) $ExpModOrderCorollary$ ▮ $Divides[o(g_1), o(g_2)]$

(6) $(Divides[o(g_2), o(g_1)]) \land (Divides[o(g_1), o(g_2)]) \land (g_1, g_2 \in \mathbb{N}^+)$ ▮ $o(g_1) = o(g_2)$

(7) ==========

(8) $\exists_{c \in G}(g_2 = c^{-1}g_1c)$ ▮ $e = {g_2}^{o(g_2)} = (c^{-1}g_1c)^{o(g_2)} = c^{-1}{g_1}^{o(g_2)}c$ ▮ $e = c^{-1}{g_1}^{o(g_2)}c$ ▮ ${g_1}^{o(g_2)} = e$

(9) $(m \in \mathbb{Z}^+) \land (m < o(g_2)) \implies \ldots$

(9.1) $e \neq {g_2}^m = (c^{-1}g_1c)^m = c^{-1}{g_1}^mc$ ▮ $e \neq c^{-1}{g_1}^mc$ ▮ $e = c * e * c^{-1} \neq {g_1}^m$ ▮ ${g_1}^m \neq e$

(10) $(m < o(g_2)) \implies (e \neq {g_1}^m)$ ▮ $\forall_{m \in \mathbb{Z}^+}((m < o(g_2)) \implies ({g_1}^m \neq e))$

(11) $({g_1}^{o(g_2)} = e) \land (\forall_{m \in \mathbb{Z}^+}((m < o(g_2)) \implies ({g_1}^m \neq e)))$ ▮ $o(g_1) = o(g_2)$

$CentralizerConjugateCosets := \forall_{c,g,h \in G}((h = c^{-1}gc) \implies (C(h) = c^{-1}C(g)c))$

(1) $(c^{-1}ac \in c^{-1}C(g)c) \implies \ldots$

(1.1) $a \in C(g) \ \blacksquare\ ag = ga$

(1.2) $(c^{-1}ac)h = (c^{-1}ac)(c^{-1}gc) = c^{-1}agc = c^{-1}gac = c^{-1}g(cc^{-1})ac = h(c^{-1}ac) \ \blacksquare\ (c^{-1}ac)h = h(c^{-1}ac) \ \blacksquare\ c^{-1}ac \in C(h)$

(2) $(c^{-1}ac \in c^{-1}C(g)c) \implies (c^{-1}ac \in C(h)) \ \blacksquare\ c^{-1}C(g)c \subseteq C(h)$

(3) $(a \in C(h)) \implies \ldots$

(3.1) $a \in C(h) \ \blacksquare\ ah = ha \ \blacksquare\ a(c^{-1}gc) = (c^{-1}gc)a$

(3.2) $(cac^{-1})g = g(cac^{-1}) \ \blacksquare\ cac^{-1} \in C(g) \ \blacksquare\ a \in c^{-1}C(g)c$

(4) $(a \in C(h)) \implies (a \in c^{-1}C(g)c) \ \blacksquare\ C(h) \subseteq c^{-1}C(g)c$

(5) $(c^{-1}C(g)c \subseteq C(h)) \wedge (C(h) \subseteq c^{-1}C(g)c) \ \blacksquare\ C(h) = c^{-1}C(g)c$

$ConjugatesMultiplicity := (g \in G) \implies (o(G) = o(C(g))|C_g|)$

(1) $\phi := \{\langle a^{-1}ga, C(g)a\rangle \in (C_g \times G : C(g))|a \in G\}$

(2) $(x, y \in G) \implies \ldots$

(2.1) $(x^{-1}gx = y^{-1}gy) \iff (gx = xy^{-1}gy) \iff (g(xy^{-1}) = (xy^{-1})g) \iff \ldots$

(2.2) $\ldots (xy^{-1} \in C(g)) \iff (C(g)(xy^{-1}) = C(g)) \iff (C(g)x = C(g)y)$

(3) $(x, y \in G) \implies ((x^{-1}gx = y^{-1}gy) \iff (C(g)x = C(g)y))$

(4) $(Func[\phi, C_g, G : C(g)]) \wedge (Inj[\phi, C_g, G : C(g)]) \wedge (Surj[\phi, C_g, G : C(g)]) \ \blacksquare\ Bij[\phi, C_g, G : C(g)]$

(5) $\exists_\phi(Bij[\phi, C_g, G : C(g)]) \ \blacksquare\ |C_g| = |G : C(g)|$

(6) $(LagrangeTheorem) \wedge (SubgroupCenter) \wedge (|C_g| = |G : C(g)|) \ \blacksquare\ o(G) = o(C(g))|G : C(g)| \ \blacksquare\ o(G) = o(C(g))|C_g|$

2.10 Normal Subgroups

$NormalSubgroup[H, G, *] := (Subgroup[H, G, *]) \wedge (\forall_{h \in H}\forall_{g \in G}(g^{-1}hg \in H))$

$CenterNormalSubgroup := NormalSubgroup[Z(G), G, *]$

(1) $SubgroupCenter \ \blacksquare\ Subgroup[Z(G), G, *]$

(2) $((h \in Z(G)) \wedge (g \in G)) \implies \ldots$

(2.1) $hg = gh \ \blacksquare\ g^{-1}hg = h \in Z(G) \ \blacksquare\ g^{-1}hg \in Z(G)$

(3) $((h \in Z(G)) \wedge (g \in G)) \implies (g^{-1}hg \in Z(G)) \ \blacksquare\ \forall_{h \in Z(G)}\forall_{g \in G}(g^{-1}hg \in Z(G))$

(4) $(Subgroup[Z(G), G, *]) \wedge (\forall_{h \in Z(G)}\forall_{g \in G}(g^{-1}hg \in Z(G))) \ \blacksquare\ NormalSubgroup[Z(G), G, *]$

$UnionConjugacyClassesNormalSubgroup := (NormalSubgroup[H, G, *]) \implies (H = \bigcup_{z \in H}(C_z))$

(1) $(NormalSubgroup[H, G, *]) \implies \ldots$

(1.1) $NormalSubgroup[H, G, *] \ \blacksquare\ \forall_{x \in H}\forall_{g \in G}(g^{-1}xg \in H)$

(1.2) $((x \in H) \wedge (y \in C_x)) \implies \ldots$

(1.2.1) $ConjugacyClassEquiv \ \blacksquare\ \exists_{c \in G}(y = c^{-1}xc)$

(1.2.2) $(\forall_{x \in H}\forall_{g \in G}(g^{-1}xg \in H)) \wedge (x \in H) \wedge (c \in G) \ \blacksquare\ y \in H$

(1.3) $((x \in H) \wedge (y \in C_x)) \implies (y \in H) \ \blacksquare\ \forall_{x \in H}(C_x \subseteq H)$

(1.4) $\forall_{x \in H}(C_x \subseteq H) \ \blacksquare\ \forall_{x \in H}\forall_y(y \in C_x \implies y \in H) \ \blacksquare\ \forall_{x \in H}\forall_y(y \notin H \implies y \notin C_x)$

(1.5) $(b \in H) \implies (b \in C_b \subseteq \bigcup_{z \in H}(C_z)) \ \blacksquare\ (b \in H) \implies (b \in \bigcup_{z \in H}(C_z))$

(1.6) $(b \notin H) \implies (\forall_{a \in H}(b \notin C_a)) \implies (b \notin \bigcup_{z \in H}(C_z)) \ \blacksquare\ (b \notin H) \implies (b \notin \bigcup_{z \in H}(C_z))$

(1.7) $((b \in H) \implies (b \in \bigcup_{z \in H}(C_z))) \wedge ((b \notin H) \implies (b \notin \bigcup_{z \in H}(C_z))) \ \blacksquare\ (b \in H) \iff (b \in \bigcup_{z \in H}(C_z))$

(1.8) $\forall_b((b \in H) \iff (b \in \bigcup_{z \in H}(C_z))) \ \blacksquare\ H = \bigcup_{z \in H}(C_z)$

(2) $(NormalSubgroup[H, G, *]) \implies (H = \bigcup_{z \in H}(C_z))$

$NormalSubgroupCosetEquiv := (NormalSubgroup[H, G, *]) \iff (\forall_{g \in G}(gH = Hg))$

(1) $CosetCardinality$ ▮ $\forall_{g\in G}(|Hg| = |gH|)$ ▮ $(\forall_{g\in G}((Hg \subseteq gH) \iff (Hg = gH)))$

(2) $(\forall_{g\in G}((Hg \subseteq gH) \iff (Hg = gH)))$ ▮ $(NormalSubgroup[H, G, *]) \iff (\forall_{h\in H}\forall_{g\in G}(g^{-1}hg \in H)) \iff \ldots$

(3) $\ldots (\forall_{h\in H}\forall_{g\in G}(hg \in gH)) \iff (\forall_{g\in G}(Hg \subseteq gH)) \iff (\forall_{g\in G}(Hg = gH))$

$NormalSubgroupIndexEquiv := (NormalSubgroup[H, G, *]) \iff (IndexSubgroup[2, H, G, *])$

(1) $NormalSubgroupCosetEquiv$ ▮ $(IndexSubgroup[2, H, G, *]) \iff (\forall_{g\in G}(gH = Hg)) \iff (NormalSubgroup[H, G, *])$

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

(1) $KernelSubgroupDomain$ ▮ $Subgroup[ker_\phi, G, *]$

(2) $((h \in ker_\phi) \wedge (g \in G)) \implies \ldots$

(2.1) $h \in ker_\phi$ ▮ $\phi(h) = e_H$

(2.2) $(Homomorphism[\phi, G, *, H, \diamond]) \wedge (InvMapsInv)$ ▮ $\phi(g^{-1} * h * g) = \phi(g^{-1}) \diamond \phi(h) \diamond \phi(g) = \phi(g)^{-1} \diamond e_H \diamond \phi(g) = e_H$

(2.3) $\phi(g^{-1} * h * g) = e_H$ ▮ $g^{-1}hg \in ker_\phi$

(3) $((h \in ker_\phi) \wedge (g \in G)) \implies (g^{-1}hg \in ker_\phi)$ ▮ $\forall_{h\in ker_\phi}\forall_{g\in G}(g^{-1}hg \in ker_\phi)$

(4) $(Subgroup[ker_\phi, G, *]) \wedge (\forall_{h\in ker_\phi}\forall_{g\in G}(g^{-1}hg \in ker_\phi))$ ▮ $NormalSubgroup[ker_\phi, G, *]$

2.11 Quotient Groups

$QuotientSet[G/H, H, G, *] := (Subgroup[H, G, *]) \wedge (G/H = \{Hg | g \in G\})$
$FactorMul[\bar{*}, H, G, *] := (Subgroup[H, G, *]) \wedge (\forall_{x,y\in G}(Hx\bar{*}Hy = \{h_1xh_2y | h_1, h_2 \in H\}))$

$QuotientGroupLemma := ((NormalSubgroup[H, G, *]) \wedge (x, y, z \in G)) \implies ((\exists_{h_1,h_2\in H}(z = h_1xh_2y)) \iff (\exists_{h_3\in H}(z = h_3xy)))$

(1) $(\exists_{h_1,h_2\in H}(z = h_1xh_2y)) \implies \ldots$

(1.1) $(Group[G, *]) \wedge (x \in G)$ ▮ $x^{-1} \in G$

(1.2) $(NormalSubgroup[H, G, *]) \wedge (x^{-1} \in G) \wedge (h_2 \in H)$ ▮ $(x^{-1})^{-1}h_2x^{-1} = xh_2x^{-1} \in H$

(1.3) $(Group[H, *]) \wedge (h_1, xh_2x^{-1} \in H)$ ▮ $h_1xh_2x^{-1} \in H$

(1.4) $(h_1xh_2x^{-1})(xy) = h_1xh_2y = z$ ▮ $(h_1xh_2x^{-1})(xy) = z$

(1.5) $(h_1xh_2x^{-1} \in H) \wedge ((h_1xh_2x^{-1})(xy) = z)$ ▮ $\exists_{h_3\in H}(z = h_3xy)$

(2) $(\exists_{h_1,h_2\in H}(z = h_1xh_2y)) \implies (\exists_{h_3\in H}(z = h_3xy))$

(3) $(\exists_{h_3\in H}(z = h_3xy)) \implies \ldots$

(3.1) $(NormalSubgroup[H, G, *]) \wedge (x \in G) \wedge (h_3 \in H)$ ▮ $x^{-1}h_3x \in H$

(3.2) $Group[H, *]$ ▮ $e \in H$

(3.3) $(e)x(x^{-1}h_3x)y = h_3xy = z$ ▮ $(e)x(x^{-1}h_3x)y = z$

(3.4) $(x^{-1}h_3x, e \in H) \wedge ((e)x(x^{-1}h_3x)y = h_3xy = z)$ ▮ $\exists_{h_1,h_2\in H}(z = h_1xh_2y)$

(4) $(\exists_{h_3\in H}(z = h_3xy)) \implies (\exists_{h_1,h_2\in H}(z = h_1xh_2y))$

(5) $((\exists_{h_1,h_2\in H}(z = h_1xh_2y)) \implies (\exists_{h_3\in H}(z = h_3xy))) \wedge ((\exists_{h_3\in H}(z = h_3xy)) \implies (\exists_{h_1,h_2\in H}(z = h_1xh_2y)))$

(6) $(\exists_{h_1,h_2\in H}(z = h_1xh_2y)) \iff (\exists_{h_3\in H}(z = h_3xy))$

$$QuotientGroup := \begin{pmatrix} ((NormalSubgroup[H, G, *]) \wedge (QuotientSet[G/H, H, G, *]) \wedge (FactorMul[\bar{*}, x, y, H, G, *])) \implies \\ (Group[G/H, \bar{*}]) \end{pmatrix}$$

(1) $(Hx, Hy \in G/H) \implies \ldots$

(1.1) $(NormalSubgroup[H, G, *]) \wedge (QuotientGroupLemma)$ ▮ $\forall_{x,y,z\in G}((\exists_{h_1,h_2\in H}(z = h_1xh_2y)) \iff (\exists_{h_3\in H}(z = h_3xy)))$

(1.2) $(z \in Hx\bar{*}Hy) \iff (\exists_{h_1,h_2\in H}(z = h_1xh_2y)) \iff (\exists_{h_3\in H}(z = h_3xy)) \iff (z \in Hxy)$ ▮ $Hx\bar{*}Hy = Hxy$

(1.3) $(Group[G, *]) \wedge (x, y \in G)$ ▮ $xy \in G$ ▮ $Hxy \in G/H$

(1.4) $(Hx\bar{*}Hy = Hxy) \wedge (Hxy \in G/H)$ ▮ $\exists!_{Hxy\in G/H}(Hx\bar{*}Hy = Hxy)$

(2) $(Hx, Hy \in G/H) \implies (\exists!_{Hxy\in G/H}(Hx\bar{*}Hy = Hxy))$ ▮ $Func[\bar{*}, G/H, G/H]$

(3) $(Hx, Hy, Hz \in G/H) \implies \ldots$

(3.1) $(Hx\bar{*}Hy)\bar{*}Hz = Hxy\bar{*}Hz = Hxyz = Hx\bar{*}Hyz = Hx\bar{*}(Hy\bar{*}Hz)$ ▮ $(Hx\bar{*}Hy)\bar{*}Hz = Hx\bar{*}(Hy\bar{*}Hz)$

(4) $(Hx, Hy, Hz \in G/H) \implies ((Hx\bar{*}Hy)\bar{*}Hz = Hx\bar{*}(Hy\bar{*}Hz))$ ▮ $\forall_{a,b,c\in G/H}((a\bar{*}b)\bar{*}c = a\bar{*}(b\bar{*}c))$

(5) $(He \in G/H) \wedge (\forall_{Hx\in G/H}(Hx\bar{*}He = Hxe = Hx = Hex = He\bar{*}Hx))$ ▮ $\exists_{e\in G/H}\forall_{a\in G/H}(a\bar{*}e = a = e\bar{*}a)$

(6) $(Hx \in G/H) \implies \ldots$

(6.1) $x \in G$ ▮ $x^{-1} \in G$ ▮ $Hx^{-1} \in G/H$

(6.2) $Hx\bar{*}Hx^{-1} = Hxx^{-1} = He = Hx^{-1}x = Hx^{-1}\bar{*}Hx$ ▮ $Hx\bar{*}Hx^{-1} = He = Hx^{-1}\bar{*}Hx$

(6.3) $(Hx^{-1} \in G/H) \wedge (Hx\bar{*}Hx^{-1} = He = Hx^{-1}\bar{*}Hx)$ ▮ $\exists_{Hx^{-1}\in G/H}(Hx\bar{*}Hx^{-1} = He = Hx^{-1}\bar{*}Hx)$

(7) $(Hx \in G/H) \implies (\exists_{Hx^{-1}\in G/H}(Hx\bar{*}Hx^{-1} = He = Hx^{-1}\bar{*}Hx))$ ▮ $\forall_{a\in G/H}\exists_{a^{-1}\in G/H}(a\bar{*}a^{-1} = e = a^{-1}\bar{*}a)$

(8) $(Func[\bar{*}, G/H, G/H]) \wedge (\forall_{a,b,c\in G/H}((a\bar{*}b)\bar{*}c = a\bar{*}(b\bar{*}c))) \wedge (\exists_{e\in G/H}\forall_{a\in G/H}(a\bar{*}e = a = e\bar{*}a)) \wedge \ldots$

(9) $\ldots (\forall_{a\in G/H}\exists_{a^{-1}\in G/H}(a\bar{*}a^{-1} = e = a^{-1}\bar{*}a))$ ▮ $Group[G/H, \bar{*}]$

$QuotientMap[\bar{\phi}, H, G, *] := (NormalSubgroup[H, G, *]) \wedge (Func[\bar{\phi}, G, *, G/H, \bar{*}]) \wedge (\forall_{g\in G}(\bar{\phi}(g) = Hg))$

$QuotientMapHomo := (QuotientMap[\bar{\phi}, H, G, *]) \implies (Homomorphism[\bar{\phi}, G, *, G/H, \bar{*}])$

(1) $QuotientMap[\bar{\phi}, H, G, *]$ ▮ $Func[\bar{\phi}, G, *, G/H, \bar{*}]$

(2) $(x, y \in G) \implies \ldots$

(2.1) $\bar{\phi}(x * y) = Hxy = Hx\bar{*}Hy = \bar{\phi}(x)\bar{*}\bar{\phi}(y)$ ▮ $\bar{\phi}(x * y) = \bar{\phi}(x)\bar{*}\bar{\phi}(y)$

(3) $(x, y \in G) \implies (\bar{\phi}(x * y) = \bar{\phi}(x)\bar{*}\bar{\phi}(y))$ ▮ $\forall_{x,y\in G}(\bar{\phi}(x)\bar{*}\bar{\phi}(y)))$

(4) $(Func[\bar{\phi}, G, *, G/H, \bar{*}]) \wedge (\forall_{x,y\in G}(\bar{\phi}(x)\bar{*}\bar{\phi}(y)))) $ ▮ $Homomorphism[\bar{\phi}, G, *, G/H, \bar{*}]$

$QuotientMapKer := (QuotientMap[\bar{\phi}, H, G, *]) \implies (ker_{\bar{\phi}} = H)$

(1) $ker_{\bar{\phi}} = \{x \in G | \bar{\phi}(x) = He\} = \{x \in G | Hx = H\} = H$

CONTHERE The proofs are omitted in these notes but you may refer to Fraleigh, pp. 229-230 $FirstIsoTheorem :=$

(1) TODO

$SecondIsoTheorem :=$

(1) TODO

$ThirdIsoTheorem :=$

(1) TODO

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

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

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

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

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

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

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

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

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

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

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

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

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

(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) $TODO = A$

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

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

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

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

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

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

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

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

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

(1) TODO

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

(1) TODO

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

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

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

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

(1) TODO

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

(1) TODO

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

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

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

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

(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) $-(A - A^T)^T = -(A^T - (A^T)^T) = -(A^T - A) = (A - A^T)$

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

(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) $(1/2) * (A_1 + {A_1}^T) = (1/2) * (A_2 + {A_2}^T)$ ▮ $A_1 = A_2$

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

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

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

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

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

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

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

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

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

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

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) $(TrivSol[\vec{X}, A]) \implies (TrivSol[LC(\vec{X}), A])$

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

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

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

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

(1) TODO

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

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

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

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

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

(6.1) $C * Z = D$

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

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

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

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

(1) Set $B = D = O$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.3 Vector Spaces

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

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

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

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

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

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

(1) $v + (-1) * v = (1 - 1) * v = 0 * v = O \blacksquare (-1) * v = -v$

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

(1) $0 * v = (0 + 0) * v = (0 * v) + (0 * v) \blacksquare O = 0 * v$

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

(1) $r * O = r * (O + O) = (r * O) + (r * O) \blacksquare O = r * O$

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

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

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

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

3.4 Subspaces and Special Subspaces

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

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

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

(1.5) $(\emptyset \neq S \subseteq V) \wedge (\forall_{r,s\in S}(r + s \in S)) \wedge (\forall_{\alpha\in\mathbb{R}}\forall_{s\in S}(\alpha * s \in S))$

(2) $(Subspace[S, V, +, *]) \implies ((\emptyset \neq S \subseteq V) \wedge (\forall_{r,s\in S}(r + s \in S)) \wedge (\forall_{\alpha\in\mathbb{R}}\forall_{s\in S}(\alpha * s \in S)))$

(3) $((\emptyset \neq S \subseteq V) \wedge (\forall_{r,s\in S}(r + s \in S)) \wedge (\forall_{\alpha\in\mathbb{R}}\forall_{s\in S}(\alpha * s \in S))) \implies \ldots$

(3.1) $((\emptyset \neq S) \wedge (\alpha, \beta \in \mathbb{R}) \wedge (u, v, w \in S)) \implies \ldots$

(3.1.1) $\emptyset \neq S$ ▮ $\exists_x(x \in V)$

(3.1.2) $(ZeroVectorGenLeft) \wedge (\forall_{\alpha\in\mathbb{R}}\forall_{s\in S}(\alpha * s \in S)) \wedge (x \in V)$ ▮ $O = 0 * x \in S$ ▮ $O \in S$

(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) $((\emptyset \neq S) \wedge (\forall_{r,s\in S}(r + s \in S)) \wedge (\forall_{\alpha\in\mathbb{R}}\forall_{s\in S}(\alpha * s \in S))) \implies (Subspace[S, V, +, *])$

(5) $(Subspace[S, V, +, *]) \iff ((\emptyset \neq S) \wedge (\forall_{r,s\in S}(r + s \in S)) \wedge (\forall_{\alpha\in\mathbb{R}}\forall_{s\in S}(\alpha * s \in S)))$

$SetSum[A + B, A, B, V, +, *] := (VectorSpace[V, +, *]) \wedge (A, B \subseteq V) \wedge (A + B = \{a + b | (a \in A) \wedge (b \in B)\})$

$$SumSubContains := \forall_{A,B,V}\left(\begin{array}{l}((Subspace[A,V,+,*]) \wedge (Subspace[B,V,+,*]) \wedge (SetSum[A+B,A,B,V,+,*])) \\ ((Subspace[A+B,V,+,*]) \wedge (A, B \subseteq A+B))\end{array} \implies \right)$$

(1) $(Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *])$ ▮ $(O \in A) \wedge (O \in B)$

(2) $(SetSum[A + B, A, B, V, +, *]) \wedge (O \in A) \wedge (O \in B)$ ▮ $O = O + O \in A + B$ ▮ $\emptyset \neq A + B$

(3) $(v \in A + B) \implies \ldots$

(3.1) $\exists_{a\in A}\exists_{b\in B}(v = a + b)$

(3.2) $(A \subseteq V) \wedge (B \subseteq V)$ ▮ $a, b \in V$

(3.3) $VectorSpace[V, +, *]$ ▮ $v = a + b \in V$

(4) $(v \in A+B) \implies (v \in V) \blacksquare A+B \subseteq V$

(5) $(\emptyset \neq A+B) \wedge (A+B \subseteq V) \blacksquare \emptyset \neq A+B \subseteq V$

(6) $(u, v \in A+B) \implies \ldots$

(6.1) $(\exists_{a_1 \in A} \exists_{b_1 \in B} (u = a_1 + b_1)) \wedge (\exists_{a_2 \in A} \exists_{b_2 \in B} (v = a_2 + b_2))$

(6.2) $u + v = (a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2)$

(6.3) $(a_1 + a_2 \in A) \wedge (b_1 + b_2 \in B) \blacksquare u + v \in A+B$

(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) $((r \in \mathbb{R}) \wedge (v \in A+B)) \implies \ldots$

(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) $(r * a \in A) \wedge (r * b) \in B \blacksquare r * v \in A+B$

(9) $((r \in \mathbb{R}) \wedge (v \in A+B)) \implies (r * v \in A+B) \blacksquare \forall_{r \in \mathbb{R}} \forall_{v \in A+B} (r * v \in A+B)$

(10) $(SubspaceEquiv) \wedge (\emptyset \neq A+B \subseteq V) \wedge (\forall_{u,v \in A+B}(u+v \in A+B)) \wedge (\forall_{r \in \mathbb{R}} \forall_{v \in A+B}(r * v \in A+B)) \blacksquare Subspace[A+B, V, +, *]$

(11) $(O \in B) \wedge (\forall_{a \in A}(a+O) = a) \blacksquare A \subseteq A+B$

(12) $(O \in A) \wedge (\forall_{b \in B}(b+O) = b) \blacksquare B \subseteq A+B$

(13) $(A \subseteq A+B) \wedge (B \subseteq A+B) \blacksquare A, B \subseteq A+B$

(14) $(Subspace[A+B, V, +, *]) \wedge (A, B \subseteq A+B)$

$$SumSubMinContains := \forall_{A,B,V} \left(\begin{array}{l} ((Subspace[A,V,+,*]) \wedge (Subspace[B,V,+,*]) \wedge (SetSum[A+B,A,B,V,+,*])) \implies \\ (\forall_C ((Subspace[C,V,+,*]) \wedge (A,B \subseteq C)) \implies (A+B \subseteq C)) \end{array} \right)$$

(1) $SumSub \blacksquare (A, B \subseteq A+B) \wedge (Subspace[A+B, V, +, *])$

(2) $((Subspace[C, V, +, *]) \wedge (A, B \subseteq C)) \implies \ldots$

(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) $(VectorSpace[C, V, +, *]) \wedge (a, b \in C) \blacksquare s = a + b \in C$

(2.2) $(s \in A+B) \implies (s \in C) \blacksquare A+B \subseteq C$

(3) $((Subspace[C, V, +, *]) \wedge (A, B \subseteq C)) \implies (A+B \subseteq C)$

$$DirSum[A \oplus B, A, B, V, +, *] := \left(\begin{array}{lll} (Subspace[A,V,+,*]) & \wedge & (Subspace[B,V,+,*]) \quad \wedge \\ (SetSum[A+B,A,B,V,+,*]) \wedge (\forall_{s \in A+B} \exists!_{\langle a,b \rangle \in A \times B} (s = a+b)) & & \end{array} \right)$$

$$DirSumEquiv := \forall_{A,B,V} \left(\begin{array}{l} ((Subspace[A,V,+,*]) \wedge (Subspace[B,V,+,*]) \wedge (SetSum[A+B,A,B,V,+,*])) \implies \\ ((DirSum[A \oplus B, A, B, V, +, *]) \iff (\exists!_{\langle a,b \rangle \in A \times B} (O = a+b))) \end{array} \right)$$

(1) $(DirSum[A \oplus B, A, B, V, +, *]) \implies \ldots$

(1.1) $(Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *]) \blacksquare (O \in A) \wedge (O \in B)$

(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) $(DirSum[A \oplus B, A, B, V, +, *]) \implies (\exists!_{\langle a,b \rangle \in A \times B} (O = a+b))$

(3) $(\exists!_{\langle a,b \rangle \in A \times B} (O = a+b)) \implies \ldots$

(3.1) $(s \in A \oplus B) \implies \ldots$

(3.1.1) $(\exists_{\langle a,b \rangle \in A \times B} (s = a+b))$

(3.1.2) $((s = a_1 + b_1) \wedge (s = a_2 + b_2)) \implies \ldots$

(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) $((a_1 - a_2 \neq O) \vee (b_1 - b_2 \neq O)) \implies (\neg \exists!_{\langle a,b \rangle \in A \times B} (O = a+b)) \implies \bot$

(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) $((s = a_1 + b_1) \wedge (s = a_2 + b_2)) \implies \langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle$

(3.1.4) $\forall_{\langle a_1,b_1 \rangle, \langle a_2,b_2 \rangle \in A \times B} (((s = a_1 + b_1) \wedge (s = a_2 + b_2)) \implies (\langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle))$

(3.1.5) $\exists_{\langle a,b \rangle \in A \times B} (s = a+b) \wedge \forall_{\langle a_1,b_1 \rangle, \langle a_2,b_2 \rangle \in A \times B} (((s = a_1 + b_1) \wedge (s = a_2 + b_2)) \implies (\langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle)) \blacksquare \exists!_{\langle a,b \rangle \in A \times B} (s = a+b)$

(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) $(\exists!_{\langle a,b\rangle\in A\times B}(O=a+b)) \implies (DirSum[A\oplus B,A,B,V,+,*])$

(5) $(DirSum[A\oplus B,A,B,V,+,*]) \iff (\exists!_{\langle a,b\rangle\in A\times B}(O=a+b))$

$$DirSumSubspace := \forall_{A,B,V}\left(\begin{array}{l}((Subspace[A,V,+,*])\wedge(Subspace[B,V,+,*])\wedge(SetSum[A+B,A,B,V,+,*])) \implies \\ ((DirSum[A\oplus B,A,B,V,+,*]) \iff (A\cap B=\{O\}))\end{array}\right)$$

(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) $(v\neq O) \implies (\neg\exists!_{\langle a,b\rangle\in A\times B}(O=a+b)) \implies \bot \blacksquare v=O$

(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) $((\langle a_1,b_1\rangle,\langle a_2,b_2\rangle\in A\times B)\wedge(O=a_1+b_1)\wedge(O=a_2+b_2)) \implies \ldots$

(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) $((\langle a_1,b_1\rangle,\langle a_2,b_2\rangle\in A\times B)\wedge(O=a_1+b_1)\wedge(O=a_2+b_2)) \implies (\langle a_1,b_1\rangle=\langle a_2,b_2\rangle)$

(3.4) $\forall_{\langle a_1,b_1\rangle,\langle a_2,b_2\rangle\in A\times B}(((O=a_1+b_1)\wedge(O=a_2+b_2)) \implies (\langle a_1,b_1\rangle=\langle a_2,b_2\rangle))$

(3.5) $(\exists_{\langle a,b\rangle\in A\times B}(O=a+b))\wedge(\forall_{\langle a_1,b_1\rangle,\langle a_2,b_2\rangle\in A\times B}(((O=a_1+b_1)\wedge(O=a_2+b_2)) \implies (\langle a_1,b_1\rangle=\langle a_2,b_2\rangle)))$

(3.6) $(\exists!_{\langle a,b\rangle\in A\times B}(O=a+b))\wedge(DirSumEquiv) \blacksquare DirSum[A\oplus B,A,B,V,+,*]$

(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

$LinComb[c,U,K,V,+,*] := (VectorSpace[V,+,*])\wedge(n\in\mathbb{N})\wedge(U\in V^n)\wedge(K\in\mathbb{R}^n)\wedge(c=\sum_{i=1}^{n}(k_i*u_i))$

$$LinSpan[S',S,V,+,*] := \left(\begin{array}{ll}(VectorSpace[V,+,*])\wedge(S\in V^n)\wedge((S=\emptyset) \implies (S'=\{O\})) & \wedge \\ ((S\neq\emptyset) \implies (S'=\{c\in V|(K\in\mathbb{R}^n)\wedge(LinComb[c,S,K,V,+,*])\}))\end{array}\right)$$

$LinSpanSubContains := \forall_{S',S,V}((LinSpan[S',S,V,+,*]) \implies ((Subspace[S',V,+,*]) \land (S \subseteq S')))$

(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) $(Subspace[S',V,+,*]) \land (S \subseteq S')$

(2) $(S = \emptyset) \implies ((Subspace[S',V,+,*]) \land (S \subseteq S'))$

(3) $(S \neq \emptyset) \implies \ldots$

(3.1) $LinSpan[S',S,V,+,*] \blacksquare S' = \{c \in V | (K \in \mathbb{R}^n) \land (LinComb[c,S,K,V,+,*])\} \blacksquare S' \subseteq V$

(3.2) $(\{0\}^n \subseteq \mathbb{R}^n) \land (LinComb[O,S,\{0\}^n,V,+,*]) \blacksquare O \in S' \blacksquare \emptyset \neq S'$

(3.3) $(S' \subseteq V) \land (\emptyset \neq S') \blacksquare \emptyset \neq S' \subseteq V$

(3.4) $(a,b \in S') \implies \ldots$

(3.4.1) $(\exists_{K_a \in \mathbb{R}^n}(LinComb[a,S,K_a,V,+,*])) \land (\exists_{K_b \in \mathbb{R}^n}(LinComb[b,S,K_b,V,+,*])) \blacksquare (a = \sum_{i=1}^n (k_{ai} * s_i)) \land (b = \sum_{i=1}^n (k_{bi} * s_i))$

(3.4.2) $a + b = \sum_{i=1}^n (k_{ai} * s_i) + \sum_{i=1}^n (k_{bi} * s_i) = \sum_{i=1}^n ((k_{ai} + k_{bi}) * s_i) \blacksquare a + b = \sum_{i=1}^n ((k_{ai} + k_{bi}) * s_i)$

(3.4.3) $\langle k_{ai} + k_{bi} | i \in \mathbb{N}_{1,n} \rangle \in \mathbb{R}^n$

(3.4.4) $(a + b = \sum_{i=1}^n ((k_{ai} + k_{bi}) * s_i)) \land (\langle k_{ai} + k_{bi} | i \in \mathbb{N}_{1,n} \rangle \in \mathbb{R}^n) \ \ldots$

(3.4.5) $\ldots \exists_{M \in \mathbb{N}^n}(a + b = \sum_{i=1}^n (m_i * s_i)) \blacksquare \exists_{M \in \mathbb{N}^n}(LinComb[a + b,S,M,V,+,*]) \blacksquare a + b \in S'$

(3.5) $(a,b \in S') \implies (a + b \in S') \blacksquare \forall_{a,b \in S'}(a + b \in S')$

(3.6) $((r \in \mathbb{R}) \land (u \in S')) \implies \ldots$

(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) $r * u = r * \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^n (r * (k_i * s_i)) = \sum_{i=1}^n (rk_i) * s_i \blacksquare r * u = \sum_{i=1}^n (rk_i) * s_i$

(3.6.3) $\langle rk_i \in \mathbb{R} | i \in \mathbb{N}_{1,n} \rangle \in \mathbb{R}^n$

(3.6.4) $(r * u = \sum_{i=1}^n (rk_i) * s_i)) \land (\langle rk_i \in \mathbb{R} | i \in \mathbb{N}_{1,n} \rangle \in \mathbb{R}^n) \blacksquare \exists_{M \in \mathbb{R}^n}(r * u = \sum_{i=1}^n (m_i * s_i))$

(3.6.5) $\exists_{M \in \mathbb{R}^n}(LinComb[r * u,S,M,V,+,*]) \blacksquare r * u \in S'$

(3.7) $((r \in \mathbb{R}) \land (u \in S')) \implies (r * u \in S') \blacksquare \forall_{r \in \mathbb{R}} \forall_{u \in S'}(r * u \in S')$

(3.8) $(SubspaceEquiv) \land (\emptyset \neq S' \subseteq V) \land (\forall_{a,b \in S'}(a + b \in S')) \land (\forall_{r \in \mathbb{R}} \forall_{u \in S'}(r * u \in S')) \blacksquare Subspace[S',V,+,*]$

(3.9) $(s_i \in S) \implies \ldots$

(3.9.1) $K_s := \left\langle \begin{cases} 1 & j = i \\ 0 & j \neq i \end{cases} | j \in \mathbb{N}_{1,n} \right\rangle \blacksquare (K_s \in \mathbb{R}^n) \land (\sum_{j=1}^n (k_{sj} * s_j) = s_i)$

(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) $(Subspace[S',V,+,*]) \land (S \subseteq S')$

(4) $(S \neq \emptyset) \implies ((Subspace[S',V,+,*]) \land (S \subseteq S'))$

(5) $((S = \emptyset) \implies ((Subspace[S',V,+,*]) \land (S \subseteq S'))) \land ((S \neq \emptyset) \implies ((Subspace[S',V,+,*]) \land (S \subseteq S'))) \ \ldots$

(6) $\ldots (Subspace[S',V,+,*]) \land (S \subseteq S')$

$LinSpanSubMinContains := \forall_{S',S,V,+,*}((LinSpan[S',S,V,+,*]) \implies (\forall_W(((Subspace[W,V,+,*]) \land (S \subseteq W)) \implies (S' \subseteq W)))$

(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) $(S \subseteq W) \land (VectorSpace[W,V,+,*]) \blacksquare s' = \sum_{i=1}^n (k_i * s_i) \in W \blacksquare s' \in W$

(2) $(s' \in S') \implies (s' \in W) \blacksquare S' \subseteq W$

$Spans[S,V,+,*] := LinSpan[V,S,V,+,*]$
$FinDim[V,+,*] := \exists_{S \in V^n}(Spans[S,V,+,*])$

$LinInd[S,V,+,*] := (VectorSpace[V,+,*]) \land (S \in V^n) \land ((S \neq \emptyset) \implies (\forall_{K \in \mathbb{R}^n}((LinComb[O,S,K,V,+,*]) \implies (K = \{0\}^n))))$

$ZeroDependent := (O \in S) \implies (\neg LinInd[S, V, +, *])$

(1) $O \in S \ \blacksquare \ \exists_{u_i \in S}(u_i = O) \ \blacksquare \ K := \langle \begin{pmatrix} \begin{cases} 1 & u_i = O \\ 0 & u_i \neq O \end{cases} | i \in \mathbb{N}_{1,n} \end{pmatrix} \rangle \ \blacksquare \ \{O\}^n \neq K \in \mathbb{R}^n$

(2) $O = \sum_{i=1}^{n}(k_i * s_i) \ \blacksquare \ LinComb[O, S, K, V, +, *]$

(3) $(LinComb[O, S, K, V, +, *]) \wedge (\{O\}^n \neq K \in \mathbb{R}^n) \ \blacksquare \ \exists_{K \in \mathbb{R}^n}((LinComb[O, S, K, V, +, *]) \wedge (K \neq \{0\}^n)) \ \blacksquare \ \neg LinInd[S, V, +, *]$

$SingletonNonZeroIndependent := (v \neq O) \implies (LinInd[\langle v \rangle, V, +, *])$

(1) $((\langle r \rangle \in \mathbb{R}^1) \wedge (LinComb[O, \langle v \rangle, \langle r \rangle, V, +, *])) \implies \ldots$

(1.1) $(ZeroVectorEquiv) \wedge (r * v = O) \ \blacksquare \ (r * v = O) \iff ((r = 0) \vee (v \neq O))$

(1.2) $v \neq O \ \blacksquare \ r = 0$

(2) $((\langle r \rangle \in \mathbb{R}^1) \wedge (LinComb[O, \langle v \rangle, \langle r \rangle, V, +, *])) \implies (r = 0) \ \blacksquare \ \forall_{r \in \mathbb{R}}((LinComb[O, \langle v \rangle, \langle r \rangle, V, +, *]) \implies (r = 0))$

(3) $LinInd[\langle v \rangle, V, +, *]$

$SubIndependent := \forall_{V,A,B} \begin{pmatrix} ((VectorSpace[V, +, *]) \wedge (A \subseteq B) \wedge (A \in V^n) \wedge (B \in V^m)) \implies \\ ((LinInd[B, V, +, *]) \implies (LinInd[A, V, +, *])) \end{pmatrix}$

(1) $((K \in \mathbb{R}^n) \wedge (LinComb[O, A, K, V, +, *])) \implies \ldots$

(1.1) $n \leq m \ \blacksquare \ L := \langle \begin{pmatrix} \begin{cases} k_j & j \leq n \\ 0 & j > n \end{cases} | j \in \mathbb{N}_{1,m} \end{pmatrix} \rangle \ \blacksquare \ L \in \mathbb{R}^m$

(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) $((K \in \mathbb{R}^n) \wedge (LinComb[O, A, K, V, +, *])) \implies (K = \{0\}^n) \ \blacksquare \ LinInd[A, V, +, *]$

$SuperDependent := \forall_{V,A,B}(((VectorSpace[V, +, *]) \wedge (A \subseteq B \subseteq V)) \implies ((\neg LinInd[A, V, +, *]) \implies (\neg LinInd[B, V, +, *])))$

(1) $\neg LinInd[A, V, +, *] \ \blacksquare \ \exists_K((LinComb[O, A, K, V, +, *]) \wedge (K \neq \{0\}^n))$

(2) $n \leq m \ \blacksquare \ L := \langle \begin{pmatrix} \begin{cases} k_j & j \leq n \\ 0 & j > n \end{cases} | j \in \mathbb{N}_{1,m} \end{pmatrix} \rangle \ \blacksquare \ L \in \mathbb{R}^m$

(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) $\exists_L((LinComb[O, B, L, V, +, *]) \wedge (L \neq \{0\}^m)) \ \blacksquare \ \neg LinInd[B, V, +, *]$

$LinDepProp := \forall_{S,V}((\neg LinInd[S, V, +, *]) \implies (\exists_{s_j \in S} \exists_{K \in \mathbb{R}^{n-1}}(LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])))$

(1) $\neg LinInd[S, V, +, *] \ \blacksquare \ \exists_{K \in \mathbb{R}^n}((LinComb[O, S, K, V, +, *]) \wedge (K \neq \{0\}^n))$

(2) $K \neq \{0\}^n \ \blacksquare \ \exists_{j \in \mathbb{N}_{1,n}}((k_j \neq 0) \wedge (\forall_{i \in \mathbb{N}_{j+1,n}}(k_i = 0))) \ \ldots$

(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) $(LinComb[O, S, K, V, +, *]) \wedge (\sum_{i=1}^{n}(k_i * s_i) = \sum_{i=1}^{j-1}(k_i * s_i) + k_j * s_j) \ \blacksquare \ O = \sum_{i=1}^{n}(k_i * s_i) = \sum_{i=1}^{j-1}(k_i * s_i) + k_j * s_j$

(5) $s_j = (-1/k_j) \sum_{i=1}^{j-1}(k_i * s_i) = \sum_{i=1}^{j-1}((-k_i/k_j) * s_i) \ \blacksquare \ s_j = \sum_{i=1}^{j-1}((-k_i/k_j) * s_i)$

(6) $\exists_{K \in \mathbb{R}^{n-1}}(LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])$

$LinDepPropCorollary := \forall_{P,S,V}(((\neg LinInd[S, V, +, *]) \wedge (LinSpan[P, S, V, +, *])) \implies (\exists_{s_j \in S}(LinSpan[P, S \setminus \{s_j\}, V, +, *])))$

(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) $\forall_{u \in P}((\exists_{K_1}(LinComb[u, S, K_1, V, +, *])) \implies (\exists_{K_2}(LinComb[u, S \setminus \{s_j\}, K_2, V, +, *]))) \ \blacksquare \ LinSpan[P, S \setminus \{s_j\}, V, +, *]$

$LinIndEquiv := \forall_{S,V}((LinInd[S, V, +, *]) \iff (\forall_{s_j \in S} \forall_{K \in \mathbb{R}^{n-1}}(\neg LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])))$

(1) $LinDepProp \blacksquare (\neg LinInd[S,V,+,*]) \implies (\exists_{s_j \in S} \exists_{K \in \mathbb{R}^{n-1}} (LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])) \ \ldots$

(2) $\ldots (\forall_{s_j \in S} \forall_{K \in \mathbb{R}^{n-1}} (\neg LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])) \implies (LinInd[S,V,+,*])$

(3) $(\exists_{s_j \in S} \exists_{K \in \mathbb{R}^{n-1}} (LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])) \implies \ldots$

(3.1) $L := \left\langle \left(\begin{cases} k_i & i \neq j \\ -1 & i = j \end{cases} \right) | i \in \mathbb{N}_{1,n} \right\rangle \blacksquare (L \in \mathbb{R}^n) \wedge (L \neq \{0\}^n)$

(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) $(LinComb[O,S,L,V,+,*]) \wedge (L \neq \{0\}^n) \blacksquare \exists_{L \in \mathbb{R}^n} ((LinComb[O,S,L,V,+,*]) \wedge (L \neq \{0\}^n)) \blacksquare (\neg LinInd[S,V,+,*])$

(4) $(\exists_{s_j \in S} \exists_{K \in \mathbb{R}^{n-1}} (LinComb[s_j, S \setminus \{s_j\}, K, V, +, *])) \implies (\neg LinInd[S,V,+,*])$

(5) $(LinInd[S,V,+,*]) \implies (\forall_{s_j \in S} \forall_{K \in \mathbb{R}^{n-1}} (\neg LinComb[s_j, S \setminus \{s_j\}, K, V, +, *]))$

(6) $(LinInd[S,V,+,*]) \iff (\forall_{s_j \in S} \forall_{K \in \mathbb{R}^{n-1}} (\neg LinComb[s_j, S \setminus \{s_j\}, K, V, +, *]))$

$LinIndSuperspace := \forall_{U,V} ((Subspace[U,V]) \implies (\forall_W ((LinInd[W,U,+,*]) \implies (LinInd[W,V,+,*]))))$

(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

$Basis[S,V,+,*] := (Spans[S,V,+,*]) \wedge (LinInd[S,V,+,*])$

$BasisEquiv := \forall_{S,V} ((Basis[S,V,+,*]) \iff (\forall_{v \in V} \exists!_{K \in \mathbb{R}^n} (LinComb[v,S,K,V,+,*]))$

(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) $((K_1, K_2 \in \mathbb{R}^n) \wedge (LinComb[v,S,K_1,V,+,*]) \wedge (LinComb[v,S,K_2,V,+,*])) \implies \ldots$

(1.1.2.1) $(v = \sum (k_{1_i} * s_i)) \wedge (v = \sum (k_{2_i} * s_i))$

(1.1.2.2) $O = v - v = \sum (k_{1_i} * s_i) - \sum (k_{2_i} * s_i) = \sum ((k_{1_i} - k_{2_i}) * s_i)$

(1.1.2.3) $L := \langle k_{1_i} - k_{2_i} | i \in \mathbb{N}_{i=1}^n \rangle \in \mathbb{R}^n$

(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) $((K_1, K_2 \in \mathbb{R}^n) \wedge (LinComb[v,S,K_1,V,+,*]) \wedge (LinComb[v,S,K_2,V,+,*])) \implies (K_1 = K_2)$

(1.1.4) $\forall_{K_1,K_2 \in \mathbb{R}^n} ((LinComb[v,S,K_1,V,+,*]) \wedge (LinComb[v,S,K_2,V,+,*]) \implies (K_1 = K_2))$

(1.1.5) $\exists!_{K \in \mathbb{R}^n} (LinComb[v,S,K,V,+,*])$

(1.2) $(v \in V) \implies (\exists!_{K \in \mathbb{R}^n} (LinComb[v,S,K,V,+,*]))$

(2) $(Basis[S,V,+,*]) \implies (\forall_{v \in V} \exists!_{K \in \mathbb{R}^n} (LinComb[v,S,K,V,+,*]))$

(3) $(\forall_{v \in V} \exists!_{K \in \mathbb{R}^n} (LinComb[v,S,K,V,+,*])) \implies \ldots$

(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) $(K \neq \{0\}^n) \implies (\neg \exists!_{K \in \mathbb{R}^n} (LinComb[O,S,K,V,+,*])) \implies \bot \blacksquare K = \{0\}^n$

(3.4) $(\exists!_{K \in \mathbb{R}^n} (LinComb[O,S,K,V,+,*])) \wedge (K = \{0\}^n) \blacksquare LinInd[S,V,+,*]$

(3.5) $(Spans[S,V,+,*]) \wedge (LinInd[S,V,+,*]) \blacksquare Basis[S,V,+,*]$

(4) $(\forall_{v \in V} \exists!_{K \in \mathbb{R}^n} (LinComb[v,S,K,V,+,*])) \implies (Basis[S,V,+,*])$

$SpanReduceBasis := \forall_{S,V} ((Spans[S,V,+,*]) \implies (\exists_B ((B \subseteq S) \wedge (Basis[B,V,+,*]))))$

(1) $LinDepPropCorollary \blacksquare \exists_B ((B \subseteq S) \wedge (LinInd[B,V,+,*]) \wedge (Spans[B,V,+,*])) \blacksquare \exists_B ((B \subseteq S) \wedge (Basis[B,V,+,*]))$

(2) TODO - formalize removing latter entries first

$FinDimBasis := \forall_V((FinDim[V,+,*]) \implies (\exists_B(Basis[B,V,+,*])))$

(1) $FinDim[V,+,*]$ ▮ $\exists_{S \in V^n}(Spans[S,V,+,*])$

(2) $(SpanReduceBasis) \wedge (Spans[S,V,+,*])$ ▮ $\exists_B(Basis[B,V,+,*])$

$LinIndExpandBasis := \forall_{L,V}((LinInd[L,V,+,*]) \implies (\exists_B((L \subseteq B) \wedge (Basis[B,V,+,*]))))$

(1) $FinDimBasis$ ▮ $\exists_C(Basis[C,V,+,*])$

(2) $S := L \cup C$

(3) $Basis[C,V,+,*]$ ▮ $Spans[C,V,+,*]$ ▮ $Spans[S,V,+,*]$

(4) $SpanReduceBasis$ ▮ $(\exists_B((B \subseteq S) \wedge (Basis[B,V,+,*]))) \wedge (L \subseteq B)$

$SpanLinIndLength := \forall_{S,T,V}(((Span[S,V,+,*]) \wedge (LinInd[T,V,+,*])) \implies (|T| \leq |S|))$

(1) $((Span[S,V,+,*]) \wedge (|T| > |S|)) \implies \ldots$

(1.1) $Span[S,V,+,*]$ ▮ $\forall_{i \in \mathbb{N}_{1,|H|}} \exists_{K_i \mathbb{R}^{|S|}}(LinComb[t_i, S, K_i V,+,*])$

(1.2) $|H| > |S|$ ▮ $\exists_{L \in \mathbb{R}^{|H|-1}}(LinComb[t_{|H|}, T \setminus \{t_{|H|}\}, L, V,+,*])$

(1.3) $L = -1 * K$ ▮ $(\sum(K+L) = O) \wedge (K+L \neq \{0\}^{|T|})$ ▮ $\neg LinInd[T,V,+,*]$

(1.4) TODO - tidy up

(2) $((Span[S,V,+,*]) \wedge (|T| > |S|)) \implies (\neg LinInd[T,V,+,*])$ ▮ $((Span[S,V,+,*]) \wedge (LinInd[T,V,+,*])) \implies (|T| \leq |S|)$

$BasisLength := \forall_{S,T,V}(((Basis[S,V,+,*]) \wedge (Basis[T,V,+,*])) \implies (|T| = |S|))$

(1) $(Span[T,V,+,*]) \wedge (LinInd[S,V,+,*])$ ▮ $|S| \leq |T|$

(2) $(Span[S,V,+,*]) \wedge (LinInd[T,V,+,*])$ ▮ $|T| \leq |S|$

(3) $(|S| \leq |T|) \wedge (|T| \leq |S|)$ ▮ $|T| = |S|$

$Dim[d,V,+,*] := ((V = \{O\}) \implies (d = 0)) \wedge ((V \neq \{O\}) \implies ((\exists_B(Basis[B,V,+,*])) \wedge (d = |B|)))$

$LinIndLengthDim := \forall_{U,V}(((LinInd[U,V,+,*]) \wedge (Dim[|U|,V,+,*])) \implies (Basis[U,V,+,*]))$

(1) $(LinIndExpandBasis) \wedge (LinInd[U,V,+,*])$ ▮ $\exists_B((U \subseteq B) \wedge (Basis[B,V,+,*]))$

(2) $(BasisLength) \wedge (Dim[|U|,V,+,*]) \wedge (Basis[B,V,+,*])$ ▮ $|B| = |U|$ ▮ $B = U$ ▮ $Basis[U,V,+,*]$

$SpanLengthDim := \forall_{U,V}(((Spans[U,V,+,*]) \wedge (Dim[|U|,V,+,*])) \implies (Basis[U,V,+,*]))$

(1) $(SpanReduceBasis) \wedge (Spans[U,V,+,*])$ ▮ $\exists_B((B \subseteq U) \wedge (Basis[B,V,+,*]))$

(2) $(BasisLength) \wedge (Dim[|U|,V,+,*]) \wedge (Basis[B,V,+,*])$ ▮ $|B| = |U|$ ▮ $B = U$ ▮ $Basis[U,V,+,*]$

$LinDepLengthDim := \forall_{U,V}(((U \subseteq V) \wedge (|U| > Dim[V])) \implies (\neg LinInd[U,V,+,*]))$

(1) Contrapositive of $BasisLinearIndCard$

(2) TODO - cleanup

$NonSpanLengthDim := \forall_{U,V}(((U \subseteq V) \wedge (|U| < Dim[V])) \implies (\neg Spans[U,V,+,*]))$

(1) Suppose $Spans[U,V,+,*]$, $B = SpanReduceBasis[U]$ to form a basis, $(|B| \leq |U| < Dim[V]) \wedge |B| = Dim[V]$ ▮ $\perp$

(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

$RankNullity := \forall_A((Matrix[A,m,n]) \implies (Rank[A] + Nullity[A] = n))$

(1) TODO

$RankInv := \forall_A((Matrix[A,m,n]) \implies ((Rank[A] = n) \iff (Inv[A])))$

(1) TODO

$RankNonTrivialSol := (\exists_X((A * X = O) \wedge (X \neq O))) \iff (Rank[A] < n)$

(1) TODO

$RankUniqueSol := (\forall_{B\in\mathcal{M}}\exists!_{X\in\mathcal{M}}(Sol[X,A,B])) \iff (Rank[A] = n)$

(1) TODO

$$SquareTheorems_8 := \forall_{A\in\mathcal{M}}\left(\begin{array}{ll} (Invertible[A]) & \iff \\ (RowEquiv[A,I_n]) & \iff \\ (\forall_X((X=O) \iff (Sol[X,A,O]))) & \iff \\ (\forall_{B\in\mathcal{M}}\exists!_{X\in\mathcal{M}}(Sol[X,A,B])) & \iff \\ (Rank[A] = n) & \iff \\ (Nullity[A] = 0) & \iff \\ \text{(The rows form a linearly independent set of vectors (to get full rank))} & \iff \\ \text{(The columns form a linearly independent set of vectors (to get full rank))} & \iff \end{array}\right)$$

3.8 Linear Transformations

$$LinTrans[L,V,+_v,*_v,W,+_w,*_w] := \left(\begin{array}{l} (Function[f,V,W]) \wedge (VectorSpace[V,+_v,*_v]) \wedge (VectorSpace[W,+_w,*_w]) \wedge \\ (\forall_{\alpha,\beta\in V}(L(\alpha +_v \beta) = L(\alpha) +_w L(\beta))) \quad \wedge \quad (\forall_{r\in\mathbb{R}}\forall_{\alpha\in V}(L(r *_v \alpha) = r *_w L(\alpha))) \end{array}\right)$$

$LinOp[L,V,+_v,*_v] := LinTrans[L,V,+_v,*_v,V,+_v,*_v]$

$\mathcal{L}[V,W] := \{L | LinTrans[L,V,+_v,*_v,W,+_w,*_w]\}$

$ZeroMapsToZero := \forall_{L,V,W}((LinTrans[L,V,+_v,*_v,W,+_w,*_w]) \implies (L(O_v) = O_w))$

(1) $L(O_v) = L(O_v +_v O_v) = L(O_v) +_w L(O_v)$

(2) $O_w = L(O_v) - L(O_v) = L(O_v)$

$SplitAddInv := \forall_{L,V,W}((LinTrans[L,V,+_v,*_v,W,+_w,*_w]) \implies (\forall_{\alpha,\beta\in V}(L(\alpha -_v \beta) = L(\alpha) -_w L(\beta))))$

(1) $L(\alpha - \beta) = L(\alpha + (-\beta)) = L(\alpha) + L(-\beta) = L(\alpha) + (-1) * L(\beta) = L(\alpha) - L(\beta)$

$$UniqBasisLT := \forall_{V,W}\left(\begin{array}{l} ((VectorSpace[V,+_v,*_v]) \wedge (VectorSpace[W,+_w,*_w]) \wedge (Basis[A,V,+_v,*_v]) \wedge (Basis[B,W,+_w,*_w])) \implies \\ (\exists!_T((LinTrans[T,V,+_v,*_v,W,+_w,*_w]) \wedge (\forall_{i\in\mathbb{N}_{1,n}}(T(a_i) = b_i)))) \end{array}\right)$$

(1) $T(\sum_{i=1}^n (k_i * a_i)) := \sum_{i=1}^n (k_i * b_i)$

(2) $(i \in \mathbb{N}_{1,n}) \implies \ldots$

(2.1) $L := \langle \begin{pmatrix} \{ & 1 & j = i \\ & 0 & j \neq i \end{pmatrix} | j \in \mathbb{N}_{1,n} \rangle$ ▮ $L \in \mathbb{R}^n$

(2.2) $T(a_i) = T(\sum_{i=1}^n (l_i * a_i)) = \sum_{i=1}^n (l_i * b_i) = b_i$ ▮ $T(a_i) = b_i$

(3) $(i \in \mathbb{N}_{1,n}) \implies (T(a_i) = b_i)$ ▮ $\forall_{i\in\mathbb{N}_{1,n}}(T(a_i) = b_i)$

(4) $(BasisEquiv) \wedge (Basis[A,V,+_v,*_v])$ ▮ $\forall_{v\in V}\exists!_{K\in\mathbb{R}^n}(LinComb[v,A,K,V,+,*])$ . . .

(5) . . . $\forall_{v_1,v_2\in V}((v_1 = v_2) \implies (T(v_1) = T(v_2)))$ ▮ $Function[T,V,W]$

(6) $(\alpha,\beta \in V) \implies \ldots$

(6.1) $(\exists_{K_\alpha}(LinComb[\alpha,A,K_\alpha,V,+_v,*_v])) \wedge (\exists_{K_\beta}(LinComb[\beta,A,K_\beta,V,+_v,*_v]))$ ▮ $(\alpha = \sum_{i=1}^n (k_{\alpha i} * a_i)) \wedge (\beta = \sum_{i=1}^n (k_{\beta_i} * a_i))$

(6.2) $T(\alpha+\beta) = T(\sum_{i=1}^n (k_{\alpha i} * a_i) + \sum_{i=1}^n (k_{\beta_i} * a_i)) = T(\sum_{i=1}^n ((k_{\alpha i} + k_{\beta_i}) * a_i))) = \sum_{i=1}^n ((k_{\alpha i} + k_{\beta_i}) * b_i) = \ldots$

(6.3) $\ldots \sum_{i=1}^{n}(k_{\alpha i} * b_i) + \sum_{i=1}^{n}(k_{\beta_i} * b_i) = T(\sum_{i=1}^{n}(k_{\alpha i} * a_i)) + T(\sum_{i=1}^{n}(k_{\beta_i} * a_i)) = T(\alpha) + T(\beta)$

(7) $(\alpha, \beta \in V) \implies (L(\alpha +_v \beta) = L(\alpha) +_w L(\beta))$ ▮ $\forall_{\alpha,\beta \in V}(L(\alpha +_v \beta) = L(\alpha) +_w L(\beta))$

(8) $((r \in \mathbb{R}) \wedge (\alpha \in V)) \implies \ldots$

(8.1) $\exists_K(LinComb[\alpha, A, K, V, +_v, *_v])$ ▮ $\alpha = \sum_{i=1}^{n}(k_i * a_i)$

(8.2) $L(r *_v \alpha) = L(r *_v \sum_{i=1}^{n}(k_i *_v a_i)) = L(\sum_{i=1}^{n}((rk_i) *_v a_i)) = \ldots$

(8.3) $\ldots \sum_{i=1}^{n}((rk_i) *_w b_i) = r *_w \sum_{i=1}^{n}(k_i *_w b_i) = r *_w L(\sum_{i=1}^{n}(k_i *_v a_i)) = r *_w L(\alpha)$

(9) $((r \in \mathbb{R}) \wedge (\alpha \in V)) \implies (L(r *_v \alpha) = r *_w L(\alpha))$ ▮ $\forall_{r \in \mathbb{R}} \forall_{\alpha \in V}(L(r *_v \alpha) = r *_w L(\alpha))$

(10) $(\forall_{i \in \mathbb{N}_{1,n}}(T(a_i) = b_i)) \wedge (Function[T, V, W]) \wedge (\forall_{\alpha,\beta \in V}(L(\alpha +_v \beta) = L(\alpha) +_w L(\beta))) \wedge (\forall_{r \in \mathbb{R}} \forall_{\alpha \in V}(L(r *_v \alpha) = r *_w L(\alpha))) \wedge \ldots$

(11) $\ldots (VectorSpace[V, +_v, *_v]) \wedge (VectorSpace[W, +_w, *_w])$ ▮ $(\forall_{i \in \mathbb{N}_{1,n}}(T(a_i) = b_i)) \wedge (LinTrans[T, V, +_v, *_v, W, +_w, *_w])$

(12) $((\forall_{i \in \mathbb{N}_{1,n}}(T_2(a_i) = b_i)) \wedge (LinTrans[T_2, V, +_v, *_v, W, +_w, *_w])) \implies \ldots$

(12.1) $\forall_{i \in \mathbb{N}_{1,n}}(T_2(a_i) = b_i)$ ▮ $\forall_{i \in \mathbb{N}_{1,n}}(T_2(c_i * a_i) = c_i * b_i)$ ▮ $T_2(\sum_{i=1}^{n}(c_i * a_i)) = \sum_{i=1}^{n}(c_i * b_i)$ ▮ $T_2 = T$

(13) $((\forall_{i \in \mathbb{N}_{1,n}}(T_2(a_i) = b_i)) \wedge (LinTrans[T_2, V, +_v, *_v, W, +_w, *_w])) \implies (T_2 = T)$

$+_{\mathcal{L}}[S + T, S, T] := (S + T)(v) = S(v) + T(v)$
$*_{\mathcal{L}}[r * T, r, T] := (r * T)(v) = r * (T(v))$
$LTVectorSpace := \forall_{V,W}(VectorSpace[\mathcal{L}[V, W], +_{\mathcal{L}}, *_{\mathcal{L}}])$

(1) TODO

$*_{\mathcal{L}}[S * T, S, T] := (S * T)(v) = S(T(v))$
$LTProdProperties := (associativity) \wedge (identity) \wedge (distributive)$

(1) TODO

$Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w] := (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (ker_L = \{\alpha \in V | L(\alpha) = O_w\})$

$KerSubspace := \forall_{L,V,W}((Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w]) \implies (Subspace[ker_L, V, +_v, *_v]))$

(1) $ZeroMapsToZero$ ▮ $L(O_v) = O_w$ ▮ $O_v \in ker_L$ ▮ $\emptyset \neq ker_L$ ▮ $\emptyset \neq ker_L \subseteq V$

(2) $(\alpha, \beta \in ker_L) \implies \ldots$

(2.1) $(L(\alpha) = O_w) \wedge (L(\beta) = O_w)$

(2.2) $L(\alpha + \beta) = L(\alpha) + L(\beta) = O_w + O_w = O_w$ ▮ $L(\alpha + \beta) \in ker_L$

(3) $(\alpha, \beta \in ker_L) \implies (\alpha + \beta \in ker_L)$ ▮ $\forall_{\alpha,\beta \in ker_L}(\alpha + \beta \in ker_L)$

(4) $((r \in \mathbb{R}) \wedge (\alpha \in ker_L)) \implies \ldots$

(4.1) $L(\alpha) = O_w$ ▮ $L(r * \alpha) = r * L(\alpha) = r * O_w = O_w$ ▮ $r * \alpha \in ker_L$

(5) $((r \in \mathbb{R}) \wedge (\alpha \in ker_L)) \implies (r * \alpha \in ker_L)$ ▮ $\forall_{r \in \mathbb{R}} \forall_{\alpha \in ker_L}(r * \alpha \in ker_L)$

(6) $(SubspaceEquiv) \wedge (\emptyset \neq ker_L \subseteq V) \wedge (\forall_{\alpha,\beta \in ker_L}(\alpha + \beta \in ker_L)) \wedge (\forall_{r \in \mathbb{R}} \forall_{\alpha \in ker_L}(r * \alpha \in ker_L))$ ▮ $Subspace[ker_L, V, +_v, *_v]$

$Rng[rng_L, L, V, +_v, *_v, W, +_w, *_w] := (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (rng_L = \{\beta \in W | \exists_{\alpha \in V}(\beta = L(\alpha))\})$

$RangeSubspace := \forall_{L,V,W}((Ran[rng_L, L, V, +_v, *_v, W, +_w, *_w]) \implies (Subspace[rng_L, W, +_w, *_w]))$

(1) $ZeroMapsToZero$ ▮ $O_w = L(O_v)$ ▮ $\exists_{\alpha \in V}(O_w = L(\alpha))$ ▮ $O_w \in rng_L$ ▮ $\emptyset \neq rng_L$ ▮ $\emptyset \neq rng_L \subseteq W$

(2) $(\alpha, \beta \in rng_L) \implies \ldots$

(2.1) $(\exists_{u \in V}(\alpha = L(u))) \wedge (\exists_{v \in V}(\beta = L(v)))$

(2.2) $\alpha + \beta = L(u) + L(v) = L(u + v)$ ▮ $\exists_{w \in V}(\alpha + \beta = L(w))$ ▮ $\alpha + \beta \in rng_L$

(3) $(\alpha, \beta \in rng_L) \implies (\alpha + \beta \in rng_L)$ ▮ $\forall_{\alpha,\beta \in rng_L}(\alpha + \beta \in rng_L)$

(4) $((r \in \mathbb{R}) \wedge (\alpha \in rng_L)) \implies \ldots$

(4.1) $\exists_{v \in V}(\alpha = L(v))$ ▮ $L(r * v) = r * L(v) = r * \alpha$ ▮ $\exists_{w \in V}(r * \alpha = L(w))$ ▮ $r * \alpha \in rng_L$

(5) $((r \in \mathbb{R}) \wedge (\alpha \in rng_L)) \implies (r * \alpha \in rng_L)$ ▮ $\forall_{r \in \mathbb{R}} \forall_{\alpha \in rng_L}(r * \alpha \in rng_L)$

(6) $(SubspaceEquiv) \wedge (\emptyset \neq rng_L \subseteq W) \wedge (\forall_{\alpha,\beta \in rng_L}(\alpha + \beta \in rng_L)) \wedge (\forall_{r \in \mathbb{R}} \forall_{\alpha \in rng_L}(r * \alpha \in rng_L))$ ▮ $Subspace[rng_L, W, +_w, *_w]$

$KerInjective := \forall_{L,V,W}((Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w]) \implies ((Injective[L, V, W]) \iff (ker_L = \{O_v\})))$

(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) $(Injective[L, V, W]) \wedge (L(O_v) = O_w) \blacksquare O_v = v$

(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) $((u, v \in V) \wedge (L(u) = L(v))) \implies \ldots$

(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) $((u, v \in V) \wedge (L(u) = L(v))) \implies (u = v) \blacksquare \forall_{u,v \in V}((L(u) = L(v)) \implies (u = v)) \blacksquare Injective[L, V, W]$

(4) $(ker_L = \{O_v\}) \implies (Injective[L, V, W])$

(5) $(Injective[L, V, W]) \iff (ker_L = \{O_v\})$

$RngSurjective := \forall_{L,V,W}((Ran[rng_L, L, V, +_v, *_v, W, +_w, *_w]) \implies ((Surjective[L, V, W]) \iff (rng_L = W)))$

(1) $(SurjEquiv) \wedge (rng(L) = rng_L) \blacksquare (Surjective[L, V, W]) \iff (rng_L = W)$

$RankNullityLT := \forall_{L,V,W}((LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \implies (Dim[V] = Dim[ker_L] + Dim[rng_L]))$

(1) $KerSubspace \blacksquare (\exists_U(Basis[U, ker_L, +_v, *_v])) \wedge (Dim[ker_L] = |U|)$

(2) $(LinIndSuperspace) \wedge (LinInd[U, ker_L, +_v, *_v]) \blacksquare LinInd[U, V, +_v, *_v]$

(3) $(LinIndExpandBasis) \wedge (LinInd[U, V, +_v, *_v]) \blacksquare (\exists_B((U \subseteq B) \wedge (Basis[B, V, +_v, *_v]))) \wedge (Dim[V] = |B|)$

(4) $U \subseteq B \blacksquare \exists_T(B = U \cup T)$

(5) $(w \in rng_L) \implies \ldots$

(5.1) $\exists_{v \in V}(w = L(v))$

(5.2) $(Basis[B, V, +_v, *_v]) \wedge (B = U \cup T) \blacksquare \exists_{K \in \mathbb{R}^{|B|}}(v = \sum_{i=1}^{|B|}(k_i * b_i) = \sum_{i=1}^{|U|}(k_i * u_i) + \sum_{i=1}^{|T|}(k_{|U|+i} * t_i))$

(5.3) $w = L(v) = L(\sum_{i=1}^{|U|}(k_i * u_i) + \sum_{i=1}^{|T|}(k_{|U|+i} * t_i)) = L(\sum_{i=1}^{|U|}(k_i * u_i)) + L(\sum_{i=1}^{|T|}(k_{|U|+i} * t_i)) = \ldots$

(5.4) $O + L(\sum_{i=1}^{|T|}(k_{|U|+i} * t_i)) = \sum_{i=1}^{|T|}(L(k_{|U|+i} * t_i)) = \sum_{i=1}^{|T|}(k_{|U|+i} * L(t_i)) \blacksquare \exists_K(LinComb[w, L(T), K, W, +, *])$

(6) $(w \in rng_L) \implies (\exists_L(LinComb[w, L(T), L, W, +, *])) \blacksquare Spans[L(T), rng_L, W, +, *]$

(7) $((K \in \mathbb{R}^n) \wedge (LinComb[O_w, L(T), K, W, +_w, *_w])) \implies \ldots$

(7.1) $O_w = \sum_{i=1}^{n}(k_i * L(t_i)) = L(\sum_{i=1}^{n}(k_i * t_i)) \blacksquare \sum_{i=1}^{n}(k_i * t_i) \in ker_L$

(7.2) $(Basis[U, ker_L, +_v, *_v]) \wedge (\sum_{i=1}^{n}(k_i * t_i) \in ker_L) \blacksquare \exists_{D \in \mathbb{R}^m}(\sum_{i=1}^{n}(k_i * t_i) = \sum_{i=1}^{m}(d_i * u_i))$

(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) $(\sum_{i=1}^{n}(k_i * t_i) = \sum_{i=1}^{m}(d_i * u_i)) \wedge (\forall_{s_j \in U \cup T} \forall_{K \in \mathbb{R}^{n-1}}(\neg LinComb[s_j, U \cup T \setminus \{s_j\}, K, V, +, *])) \blacksquare (D = \{O\}) \wedge (K = \{O\})$

(8) $((K \in \mathbb{R}^n) \wedge (LinComb[O_w, L(T), K, W, +_w, *_w])) \implies (K = \{O\}) \blacksquare LinInd[L(T), W, +_w, *_w]$

(9) $(SubIndependent) \wedge (LinInd[L(T), W, +_w, *_w]) \blacksquare LinInd[L(T), rng_L, +_w, *_w]$

(10) $(Spans[L(T), rng_L, W, +, *]) \wedge (LinInd[L(T), rng_L, +_w, *_w]) \blacksquare Basis[L(T), rng_L, +_w, *_w] \blacksquare Dim[rng_L] = |L(T)| = |T|$

(11) $B = U \cup T \blacksquare |B| = |U| + |T| \blacksquare Dim[V] = Dim[ker_L] + Dim[rng_L]$

$$InjectiveSurjectiveEqualDim := \forall_{T,V,W}\left(\begin{array}{l} ((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \wedge (Dim[V] = Dim[W]) \wedge (Injective[T, V, W])) \implies \\ (Surjective[T, V, W]) \end{array} \right)$$

(1) $(KerInjective) \wedge (Injective[T, V, W]) \blacksquare ker_T = \{O\} \blacksquare Dim[ker_T] = 0$

(2) $(RankNullityLT) \wedge (Dim[ker_T] = 0) \blacksquare Dim[V] = Dim[ker_T] + Dim[rng_T] = Dim[rng_T] \blacksquare Dim[V] = Dim[rng_T]$

(3) $(Dim[V] = Dim[W]) \wedge (Dim[V] = Dim[rng_T]) \blacksquare Dim[W] = Dim[rng_T]$

(4) $RangeSubspace \blacksquare Subspace[rng_T, W, +_w, *_w]$

(5) $(Subspace[rng_T, W, +_w, *_w]) \wedge (Dim[W] = Dim[rng_T]) \blacksquare \exists_B((Basis[B, W, +_w, *_w]) \wedge (Basis[B, rng_T, +_w, *_w]))$

(6) $(Spans[W] = Spans[rng_T]) \blacksquare W = rng_T \blacksquare Surjective[T, V, W]$

$$SurjectiveInjectiveEqualDim := \forall_{T,V,W}\left(\begin{array}{l} ((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \wedge (Dim[V] = Dim[W]) \wedge (Surjective[T, V, W])) \implies \\ (Injective[T, V, W]) \end{array} \right)$$

(1) $RankNullityLT \blacksquare Dim[V] = Dim[ker_T] + Dim[rng_T]$

(2) $Surjective[T, V, W] \blacksquare rng_T = W \blacksquare Dim[rng_T] = Dim[W]$

(3) $(Dim[V] = Dim[W]) \wedge (Dim[V] = Dim[ker_T] + Dim[rng_T]) \wedge (Dim[rng_T] = Dim[W]) \blacksquare Dim[ker_T] + Dim[rng_T] = Dim[rng_T] \blacksquare Dim[ker_T] = 0 \blacksquare ker_T = \{O\}$

(4) $(KerInjective) \wedge (er_T = \{O\}) \blacksquare Injective[T, V, W]$

$$SmallerMapNotInjective := \forall_{T,V,W}(((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \wedge (Dim[V] > Dim[W])) \implies (\neg Injective[T, V, W]))$$

(1) $(RankNullityLT) \wedge (Dim[W] \geq Dim[rng_T]) \blacksquare Dim[ker_T] = Dim[V] - Dim[rng_T] \geq Dim[V] - Dim[W] > 0 \blacksquare Dim[ker_T] \neq 0$

(2) $(KerInjective) \wedge (Dim[ker_T] \neq 0) \blacksquare \neg Injective[T, V, W]$

$$LargerMapNotSurjective := \forall_{T,V,W}(((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \wedge (Dim[V] < Dim[W])) \implies (\neg Surjective[T, V, W]))$$

(1) $RankNullityLT \blacksquare Dim[rng_T] = Dim[V] - Dim[ker_T] \leq Dim[V] < Dim[W]$

(2) $Dim[rng_T] < Dim[W] \blacksquare Dim[rng_T] \neq Dim[W] \blacksquare \neg Surjective[T, V, W]$

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

$$LTInv[L^{-1}, L, V, +_v, *_v, W, +_w, *_w] := \left(\begin{array}{ccc} (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (LinTrans[L^{-1}, W, +_w, *_w, V, +_v, *_v]) \wedge \\ (L^{-1} \circ L = 1_v) & \wedge & (L \circ L^{-1} = 1_w) \end{array} \right)$$

$$LTInvUniq := \forall_{L_1^{-1}, L_2^{-1}}(((LTInv[L_1^{-1}, L, V, +_v, *_v, W, +_w, *_w]) \wedge (LTInv[L_2^{-1}, L, V, +_v, *_v, W, +_w, *_w])) \implies (L_1^{-1} = L_2^{-1}))$$

(1) $L_1^{-1} = L_1^{-1} \circ 1_w = L_1^{-1} \circ (L \circ L_2^{-1}) = (L_1^{-1} \circ L) \circ L_2^{-1} = 1_v \circ L_2^{-1} = L_2^{-1} \blacksquare L_1^{-1} = L_2^{-1}$

$$LTInvertible[L, V, +_v, *_v, W, +_w, *_w] := \exists_{L^{-1}}(LTInv[L^{-1}, L, V, +_v, *_v, W, +_w, *_w])$$

$$InvertibleBijectiveEquiv := \forall_L((LTInvertible[L, V, +_v, *_v, W, +_w, *_w]) \iff ((Injective[L, V, W]) \wedge (Surjective[L, V, W])))$$

(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) $(L(u) = L(w)) \implies \ldots$

(1.2.1) $u = L^{-1}(L(u)) = L^{-1}(L(v)) = v \blacksquare u = v$

(1.3) $(L(u) = L(w)) \implies (u = w) \blacksquare \forall_{u,w}((L(u) = L(w)) \implies (u = w)) \blacksquare Injective[L, V, W]$

(1.4) $(w \in W) \implies \ldots$

(1.4.1) $L^{-1}(w) \in V$

(1.4.2) $L \circ L^{-1} = 1_w \blacksquare L(L^{-1}(w) = w)$

(1.4.3) $(L^{-1}(w) \in V) \wedge (L(L^{-1}(w) = w)) \blacksquare \exists_{v \in V}(w = (L(v)))$

(1.5) $(w \in W) \implies (\exists_{v \in V}(w = (L(v)))) \blacksquare \forall_{w \in W} \exists_{v \in V}(w = L(v)) \blacksquare Surjective[L, V, W]$

(1.6) $(Injective[L, V, W]) \wedge (Surjective[L, V, W])$

(2) $(LTInvertible[L,V,+_v,*_v,W,+_w,*_w]) \implies ((Injective[L,V,W]) \wedge (Surjective[L,V,W]))$

(3) $((Injective[L,V,W]) \wedge (Surjective[L,V,W])) \implies \ldots$

(3.1) $(Injective[L,V,W]) \wedge (Surjective[L,V,W])$ ▮ $\forall_{w \in W} \exists!_{v \in V} (w = L(v))$

(3.2) $S := \{(w,v) \in W \times V | w = L(v)\}$

(3.3) $(\forall_{w \in W} \exists!_{v \in V} (w = L(v))) \wedge (S = \{(w,v) \in W \times V | w = L(v)\})$ ▮ $Function[S,W,V]$

(3.4) $(\forall_{v \in V} (S(L(v)) = v)) \wedge (\forall_{w \in W} (L(S(w)) = w))$

(3.5) $(w_1, w_2 \implies W) \implies \ldots$

(3.5.1) $(LinTrans[L,V,+_v,*_v,W,+_w,*_w]) \wedge (\forall_{w \in W} (L(S(w)) = w))$ ▮ $L(S(w_1) + S(w_2)) = L(S(w_1)) + L(S(w_2)) = w_1 + w_2$

(3.5.2) $(\forall_{w \in W} (L(S(w)) = w)) \wedge (w_1 + w_2 \in W)$ ▮ $L(S(w_1 + w_2)) = w_1 + w_2$

(3.5.3) $L(S(w_1) + S(w_2)) = w_1 + w_2 = L(S(w_1 + w_2))$ ▮ $L(S(w_1) + S(w_2)) = L(S(w_1 + w_2))$

(3.5.4) $(Injective[L,V,W]) \wedge (L(S(w_1) + S(w_2)) = L(S(w_1 + w_2)))$ ▮ $S(w_1) + S(w_2) = S(w_1 + w_2)$

(3.6) $(w_1, w_2 \implies W) \implies (S(w_1 + w_2) = S(w_1) + S(w_2))$ ▮ $\forall_{w_1, w_2 \in W} (S(w_1 + w_2) = S(w_1) + S(w_2))$

(3.7) $((r \in \mathbb{R}) \wedge (w \in W)) \implies \ldots$

(3.7.1) $(LinTrans[L,V,+_v,*_v,W,+_w,*_w]) \wedge (\forall_{w \in W} (L(S(w)) = w))$ ▮ $L(r * S(w)) = r * L(S(w)) = r * w$

(3.7.2) $(\forall_{w \in W} (L(S(w)) = w)) \wedge (r * w \in W)$ ▮ $L(S(r * w)) = r * w$

(3.7.3) $L(r * S(w)) = r * w = L(S(r * w))$ ▮ $L(r * S(w)) = L(S(r * w))$

(3.7.4) $(Injective[L,V,W]) \wedge (L(r * S(w)) = L(S(r * w)))$ ▮ $r * S(w) = S(r * w)$

(3.8) $((r \in \mathbb{R}) \wedge (w \in W)) \implies (r * S(w) = S(r * w))$ ▮ $\forall_{r \in \mathbb{R}} \forall_{w \in W} (S(r * w) = r * S(w)$

(3.9) $(Function[S,W,V]) \wedge (\forall_{w_1, w_2 \in W} (S(w_1 + w_2) = S(w_1) + S(w_2))) \wedge (\forall_{r \in \mathbb{R}} \forall_{w \in W} (S(r * w) = r * S(w)))$

(3.10) $LinTrans[S,W,+_w,*_w,V,+_v,*_v]$

(3.11) $\forall_{v \in V} ((S(L(v)) = v))$ ▮ $S \circ L = 1_v$

(3.12) $\forall_{w \in W} (L(S(w)) = w)$ ▮ $L \circ S = 1_w$

(3.13) $(LinTrans[S,W,+_w,*_w,V,+_v,*_v]) \wedge (S \circ L = 1_v) \wedge (L \circ S = 1_w)$ ▮ $LTInv[S,L,V,+_v,*_v,W,+_w,*_w]$

(3.14) $\exists_{L^{-1}} (LTInv[L^{-1},L,V,+_v,*_v,W,+_w,*_w])$ ▮ $LTInvertible[L,V,+_v,*_v,W,+_w,*_w]$

(4) $((Injective[L,V,W]) \wedge (Surjective[L,V,W])) \implies (LTInvertible[L,V,+_v,*_v,W,+_w,*_w])$

(5) $(LTInvertible[L,V,+_v,*_v,W,+_w,*_w]) \iff ((Injective[L,V,W]) \wedge (Surjective[L,V,W]))$

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

$CoordVec[[\alpha]_S, \alpha, S, V, +, *] := (Basis[S,V,+,*]) \wedge (S * [\alpha]_S = \alpha \in V)$

$$LTMatrix := \forall_{L,V,W} \left(\begin{array}{l} ((LinTrans[L,V,+_v,*_v,W,+_w,*_w]) \wedge (Basis[A,V,+_v,*_v]) \wedge (Basis[B,W,+_w,*_w])) \implies \\ (\forall_{v \in V} (CoordVec[[L(v)]_B, L(v), B, W, +_w, *_w] = \langle [L(a_i)]_B | a_i \in A \rangle * CoordVec[[v]_A, v, A, V, +_v, *_v])) \end{array} \right)$$

(1) $Basis[A,V,+_v,*_v]$ ▮ $\exists_{K \in \mathbb{R}^n} (v = \sum_{i=1}^n (k_i * a_i))$ ▮ $K^T = CoordVec[[v]_A, , v, A, V, +, *]$

(2) $[L(v)]_B = [L(\sum_{i=1}^n (k_i * a_i))]_B = [\sum_{i=1}^n (L(k_i * a_i))]_B = \sum_{i=1}^n ([L(k_i * a_i)]_B) = \sum_{i=1}^n ([k_i * L(a_i)]_B) = \sum_{i=1}^n (k_i * [L(a_i)]_B) = \ldots$

(3) $\ldots \langle [L(a)]_B | a \in A \rangle * K^T = \langle [L(a)]_B | a \in A \rangle * [v]_A$ ▮ $[L(v)]_B = \langle [L(a)]_B | a \in A \rangle * [v]_A$

Note: Shorthand is to RREF the augmented matrix [Columns of B | Columns of A] into [I | M], thus M is the transition matrix

$$TransitionMatrix := \forall_{L,V} \left(\begin{array}{l} ((Basis[A,V,+,*]) \wedge (Basis[B,V,+,*])) \\ (\forall_{v \in V} (CoordVec[[v]_B, v, B, W, +_w, *_w] = \langle [a]_B | a \in A \rangle * CoordVec[[v]_A, v, A, V, +_v, *_v])) \end{array} \implies \right)$$

(1) $(LTMatrix) \wedge (LinTrans[I,V,+,*,V,+,*])$ ▮ $[I(v)]_B = \langle [I(a)]_B | a \in A \rangle * [v]_A$ ▮ $[v]_B = \langle [a]_B | a \in A \rangle * [v]_A$

$LTOverTransition := (([L(a)]_T = A * [a]_S) \wedge (P * [a]_{S'} = [a]_S) \wedge (Q * [L(a)]_{T'} = [L(a)]_T)) \implies ([L(a)]_{T'} = (Q^{-1} * A * P) * [a]_{S'})$

(1) $[L(a)]_{T'} = Q^{-1} * [L(a)]_T = Q^{-1} * A * [a]_S = Q^{-1} * A * P * [a]_{S'}$ ▮ $[L(a)]_{T'} = (Q^{-1} * A * P) * [a]_{S'}$

$LOOverTransition := (([L(a)]_S = A * [a]_S) \wedge (P * [a]_{S'} = [a]_S)) \implies ([L(a)]_{S'} = (P^{-1} * A * P) * [a]_{S'})$

(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

$SimMatrix[A, B] := \exists_P (B = P * A * P^{-1})$

$SimMatrixEquiv := (SimMatrix[A, B]) \iff (\exists_{S,T,S',T}(([L(a)]_T = A * [a]_S) \wedge ([L(a)]_{T'} = B * [a]_{S'})))$

(1) TODO

$SimRank := (SimMatrix[A, B]) \implies (Rank[A] = Rank[B])$

(1) TODO

3.10 Determinants

$Perm[\sigma, S] := Bij[\sigma, S, S]$
$IntPermSet[S_n, n] := S_n = \{\sigma | Perm[\sigma, \mathbb{N}_{1,n}]\}$

$IntPermSetCard := (IntPermSet[S_n, n]) \implies (|S_n| = n!)$

(1) TODO: Combinatorics / induction on N

$IntPermGroup := Group[S_n, \circ]$

(1) $Perm[I_n, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \ \blacksquare\ I_n \in S_n$

(2) $(\sigma, \tau, \upsilon \in S_n) \implies \ldots$

(2.1) $(Bij[\sigma, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}]) \wedge (Bij[\tau, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}]) \ \blacksquare\ Bij[\sigma \circ \tau, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \ \blacksquare\ \sigma \circ \tau \in S_n$

(2.2) $(Bij[\sigma, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}]) \wedge (Bij[\tau, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}]) \wedge (Bij[\upsilon, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}]) \ \blacksquare\ (\sigma \circ \tau) \circ \upsilon = \sigma \circ (\tau \circ \upsilon)$

(2.3) $\sigma \circ I_n = \sigma = I_n \circ \sigma$

(2.4) $Bij[\sigma, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \ \blacksquare\ \sigma \circ \sigma^{-1} = I_n = \sigma^{-1} \circ \sigma$

(3) $Group[S_n, \circ]$

$IntPermSetDecomp := (IntPermSet[S_n, n]) \wedge (Perm[\tau, \mathbb{N}_{1,n}]) \implies (S_n = \{\tau \circ \sigma | \sigma \in S_n\} = \{\sigma \circ \tau | \sigma \in S_n\})$

(1) $(\sigma \in S_n) \iff ()$