

# Contents



# Chapter 1

## Real Analysis

(1.5)

$$\begin{aligned} \text{OrderTrichotomy}[\prec, S] &:= \forall_{x,y \in S} (x < y \vee x = y \vee y < x) \\ \text{OrderTransitivity}[\prec, S] &:= \forall_{x,y,z \in S} ((x < y \wedge y < z) \implies x < z) \\ \text{Order}[\prec, S] &:= (\text{OrderTrichotomy}[\prec, S]) \wedge (\text{OrderTransitivity}[\prec, S]) \end{aligned}$$

(1.7)

$$\begin{aligned} \text{BoundedAbove}[E, S, \prec] &:= (\text{Order}[\prec, S]) \wedge (E \subset S) \wedge \left( \exists_{\beta \in S} \forall_{x \in E} (x \leq \beta) \right) \\ \text{BoundedBelow}[E, S, \prec] &:= (\text{Order}[\prec, S]) \wedge (E \subset S) \wedge \left( \exists_{\beta \in S} \forall_{x \in E} (\beta \leq x) \right) \\ \text{UpperBound}[\beta, E, S, \prec] &:= (\text{Order}[\prec, S]) \wedge (E \subset S) \wedge (\beta \in S \wedge \forall_{x \in E} (x \leq \beta)) \\ \text{LowerBound}[\beta, E, S, \prec] &:= (\text{Order}[\prec, S]) \wedge (E \subset S) \wedge (\beta \in S \wedge \forall_{x \in E} (\beta \leq x)) \end{aligned}$$

(1.8)

$$\begin{aligned} \text{LUB}[\alpha, E, S, \prec] &:= (\text{UpperBound}[\alpha, E, S, \prec]) \wedge \left( \forall_{\gamma} (\gamma < \alpha \implies \neg \text{UpperBound}[\gamma, E, S, \prec]) \right) \\ \text{GLB}[\alpha, E, S, \prec] &:= (\text{LowerBound}[\alpha, E, S, \prec]) \wedge \left( \forall_{\beta} (\alpha < \beta \implies \neg \text{LowerBound}[\beta, E, S, \prec]) \right) \end{aligned}$$

(1.10)

$$\begin{aligned} \text{LUBProperty}[S, \prec] &:= \forall_E \left( ((\emptyset \neq E \subset S) \wedge (\text{BoundedAbove}[E, S, \prec]) \implies \exists_{\alpha \in S} (\text{LUB}[\alpha, E, S, \prec])) \right) \\ \text{GLBProperty}[S, \prec] &:= \forall_E \left( ((\emptyset \neq E \subset S) \wedge (\text{BoundedBelow}[E, S, \prec]) \implies \exists_{\alpha \in S} (\text{GLB}[\alpha, E, S, \prec])) \right) \end{aligned}$$

(1.11)

$$\text{LUBPropertyImpliesGLBProperty} := \text{LUBProperty}[S, \prec] \implies \text{GLBProperty}[S, \prec]$$

(1)  $\text{LUBProperty}[S, \prec] \implies \dots$

wts: 2

(1.1)  $(\emptyset \neq B \subset S \wedge \text{BoundedBelow}[B, S, \prec]) \implies \dots$

wts: 1.2

(1.1.1)  $\text{Order}[\prec, S] \wedge \exists_{\delta' \in S} (\text{LowerBound}[\delta', B, S, \prec])$

from: [BoundedBelow](#), 1.1

(1.1.2)  $|B| = 1 \implies \dots$

wts: 1.1.3

(1.1.2.1)  $\exists_{u'} (u' \in B) \blacksquare u := \text{choice}(\{u' : u' \in B\}) \blacksquare B = \{u\}$

from: 1.1.2

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

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

(1.1.4)  $|B| \neq 1 \implies \dots$

wts: 1.1.5

(1.1.4.1)  $\forall_E ((\emptyset \neq E \subset S \wedge \text{BoundedAbove}[E, S, \prec]) \implies \exists_{\alpha \in S} (\text{LUB}[\alpha, E, S, \prec]))$

from: [LUBProperty](#), 1

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

(1.1.4.3)  $|B| > 1 \wedge \text{OrderTrichotomy}[\prec, S] \blacksquare \exists_{b_1' \in B} \exists_{b_0' \in B} (b_0' < b_1')$

from: [Order](#), 1.1.1  
wts: 1.1.4.7

(1.1.4.4)  $b_1 := \text{choice}(\{b_1' \in B : \exists_{b_0' \in B} (b_0' < b_1')\}) \blacksquare \neg \text{LowerBound}[b_1, B, S, \prec]$

from: 1.1.4.2

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

(1.1.4.6)  $\delta := \text{choice}(\{\delta' \in S : \text{LowerBound}[\delta', B, S, \prec]\}) \blacksquare \delta \in L \blacksquare \emptyset \neq L$

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)  $\forall_{y \in L} (\text{LowerBound}[y_0, B, S, \prec]) \blacksquare \forall_{y \in L} \forall_{x \in B} (y_0 \leq x)$

from: [LowerBound](#), 1.1.4.2  
wts: 1.1.4.10

$$(1.1.4.9) \quad \forall_{x \in B} \left( x \in S \wedge \forall_{y \in L} (y_0 \leq x) \right) \quad \blacksquare \quad \forall_{x \in B} (\text{UpperBound}[x, L, S, <])$$

from: *UpperBound*

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

$$(1.1.4.11) \quad \emptyset \neq L \subset S \wedge \text{BoundedAbove}[L, S, <]$$

from: 1.1.4.7, 1.1.4.10

$$(1.1.4.12) \quad \exists_{\alpha' \in S} (\text{LUB}[\alpha', L, S, <]) \quad \blacksquare \quad \alpha := \text{choice}(\{\alpha' \in S : (\text{LUB}[\alpha', L, S, <])\})$$

from: 1.1.4.1  
wts: 1.1.4.21

$$(1.1.4.13) \quad \forall_x (x \in B \implies \text{UpperBound}[x, L, S, <])$$

from: 1.1.4.9  
wts: 1.1.4.17

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

$$(1.1.4.15) \quad \gamma < \alpha \implies \dots$$

wts: 1.1.4.16

$$(1.1.4.15.1) \quad \neg \text{UpperBound}[\gamma, L, S, <] \quad \blacksquare \quad \gamma \notin B$$

from: *LUB*, 1.1.4.12, 1.1.4.14

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

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

from: *LowerBound*

$$(1.1.4.18) \quad \alpha < \beta \implies \dots$$

wts: 1.1.4.19

$$(1.1.4.18.1) \quad \forall_{y \in L} (y_0 \leq \alpha < \beta) \quad \blacksquare \quad \forall_{y \in L} (y_0 \neq \beta)$$

from: *LUB*, 1.1.4.12, 1.1.4.18

$$(1.1.4.18.2) \quad \beta \notin L \quad \blacksquare \quad \neg \text{LowerBound}[\beta, B, S, <]$$

from: 1.1.4.2

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

$$(1.1.4.20) \quad \text{LowerBound}[\alpha, B, S, <] \wedge \forall_{\beta \in S} (\alpha < \beta \implies \neg \text{LowerBound}[\beta, B, S, <])$$

from: 1.1.4.17, 1.1.4.19

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

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

$$(1.1.6) \quad \left( |B| = 1 \implies \exists_{\epsilon_0 \in S} (\text{GLB}[\epsilon_0, B, S, <]) \right) \wedge \left( |B| \neq 1 \implies \exists_{\epsilon_1 \in S} (\text{GLB}[\epsilon_1, B, S, <]) \right)$$

from: 1.1.3, 1.1.5

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

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

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

$$(1.4) \quad \text{GLBProperty}[S, <]$$

$$(2) \quad \text{LUBProperty}[S, <] \implies \text{GLBProperty}[S, <]$$

$$(1.12)$$

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

$$\text{***** (Field}[F, +, *] \wedge x, y, z \in F) \implies \dots \text{*****}$$

$$(1.14)$$

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

$$(1) \quad y = 0 + y = (x + (-x)) + y = ((-x) + x) + y = (-x) + (x + y) = \dots$$

from: *Field*

$$(2) \quad (-x) + (x + z) = ((-x) + x) + z = (x + (-x)) + z = 0 + z = z$$

from: *Field*

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

$$(1) \quad x + y = x = 0 + x = x + 0$$

from: *Field*

$$(2) \quad y = 0$$

from: *AdditiveCancellation*

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

$$(1) \quad x + y = 0 = x + (-x)$$

from: *Field*

$$(2) \quad y = -x$$

from: *AdditiveCancellation*

$$\text{DoubleNegative} := x = -(-x)$$

$$(1) \quad 0 = x + (-x) = (-x) + x \quad \blacksquare \quad 0 = (-x) + x$$

from: *Field*

$$(2) \quad x = -(-x)$$

from: [AdditiveInverseUniqueness](#)

(1.15)

$$\textcolor{red}{\textit{MultiplicativeCancellation}} := (x \neq 0 \wedge x * y = x * z) \implies y = z \quad \text{---}$$

$$\textcolor{red}{\textit{MultiplicativeIdentityUniqueness}} := (x \neq 0 \wedge x * y = x) \implies y = 1 \quad \text{---}$$

$$\textcolor{red}{\textit{MultiplicativeInverseUniqueness}} := (x \neq 0 \wedge x * y = 1) \implies y = 1/x \quad \text{---}$$

$$\textcolor{red}{\textit{DoubleReciprocal}} := (x \neq 0) \implies x = 1/(1/x) \quad \text{---}$$

(1.16)

$$\textcolor{red}{\textit{Domination}} := 0 * x = 0$$

from: [Field](#)

$$(1) \quad 0 * x = (0 + 0) * x = 0 * x + 0 * x \quad \blacksquare \quad 0 * x = 0 * x + 0 * x$$

$$(2) \quad 0 * x = 0$$

from: [AdditiveIdentityUniqueness](#)

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

$$(1) \quad (x \neq 0 \wedge y \neq 0) \implies \dots$$

$$(1.1) \quad (x * y = 0) \implies \dots$$

$$(1.1.1) \quad 1 = 1 * 1 = (x * (1/x)) * (y * (1/y)) = (x * y) * ((1/x) * (1/y)) = 0 * ((1/x) * (1/y)) = 0$$

from: [Field](#), [Domination](#), 1, 1.1

$$(1.1.2) \quad 1 = 0 \wedge 1 \neq 0 \quad \blacksquare \quad \perp$$

from: [Field](#)

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

$$(2) \quad (x \neq 0 \wedge y \neq 0) \implies x * y \neq 0$$

$$\textcolor{red}{\textit{NegationCommutativity}} := (-x) * y = -(x * y) = x * (-y)$$

$$(1) \quad x * y + (-x) * y = (x + -x) * y = 0 * y = 0 \quad \blacksquare \quad x * y + (-x) * y = 0$$

from: [Field](#), [Domination](#)  
wts: 2

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

from: [AdditiveInverseUniqueness](#)

$$(3) \quad x * y + x * (-y) = x * (y_0 + -y) = x * 0 = 0 \quad \blacksquare \quad x * y + x * (-y) = 0$$

from: [Field](#), [Domination](#)  
wts: 4

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

from: [AdditiveInverseUniqueness](#)

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

from: 2, 4

$$\textcolor{red}{\textit{NegativeMultiplication}} := (-x) * (-y) = x * y$$

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

from: [NegationCommutativity](#), [DoubleNegative](#)

(1.17)

$$\textcolor{red}{\textit{OrderedField}}[F, +, *, <] := \left( \begin{array}{l} \textcolor{teal}{\textit{Field}}[F, +, *] \quad \wedge \quad \textcolor{teal}{\textit{Order}}[<, F] \quad \wedge \\ \forall_{x,y,z \in F} (y_0 < z \implies x + y < x + z) \quad \wedge \\ \forall_{x,y \in F} ((x > 0 \wedge y > 0) \implies x * y > 0) \end{array} \right)$$

$$\text{*****} (\textcolor{teal}{\textit{OrderedField}}[F, +, *, <] \wedge x, y, z \in F) \implies \dots \text{*****}$$

(1.18)

$$\textcolor{red}{\textit{NegationOnOrder}} := x > 0 \iff -x < 0$$

$$(1) \quad x > 0 \implies \dots$$

$$(1.1) \quad 0 = (-x) + x > (-x) + 0 = -x \quad \blacksquare \quad 0 > -x \quad \blacksquare \quad -x < 0$$

from: [OrderedField](#)

$$(2) \quad x > 0 \implies -x < 0$$

$$(3) \quad -x < 0 \implies \dots$$

$$(3.1) \quad 0 = x + (-x) < x + 0 = x \quad \blacksquare \quad 0 < x \quad \blacksquare \quad x > 0$$

from: [OrderedField](#)

$$(4) \quad -x < 0 \implies x > 0$$

$$(5) \quad x > 0 \implies -x < 0 \wedge -x < 0 \implies x > 0 \quad \blacksquare \quad x > 0 \iff -x < 0$$

from: 2, 4

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

$$(1) \quad (x > 0 \wedge y < z) \implies \dots$$

$$(1.1) \quad (-y) + z > (-y) + y = 0 \quad \blacksquare \quad z + (-y) = 0$$

from: [OrderedField](#)

$$(1.2) \quad x * (z + (-y)) > 0 \quad \blacksquare \quad x * z + x * (-y) > 0$$

from: [OrderedField](#)

$$(1.3) \quad x * z = 0 + x * z = (x * y + -(x * y)) + x * z = (x * y + x * (-y)) + x * z = \dots$$

from: *Field, NegationCommutativity*

$$(1.4) \quad x * y + (x * z + x * (-y)) > x * y + 0 = x * y$$

from: *Field, 1.2*

$$(1.5) \quad x * z > x * y$$

from: 1.3, 1.4

$$(2) \quad (x > 0 \wedge y < z) \implies x * z > x * y$$

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

$$(1) \quad (x < 0 \wedge y < z) \implies \dots$$

$$(1.1) \quad -x > 0$$

from: *NegationOnOrder*

$$(1.2) \quad (-x) * y < (-x) * z \quad \blacksquare \quad 0 = x * y + (-x) * y < x * y + (-x) * z \quad \blacksquare \quad 0 < x * y + (-x) * z$$

from: *PositiveFactorPreservesOrder*

$$(1.3) \quad 0 < (-x) * (-y + z) \quad \blacksquare \quad 0 > x * (-y + z) \quad \blacksquare \quad 0 > -(x * y) + x * z$$

from: *NegationOnOrder*

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

$$(2) \quad (x < 0 \wedge y < z) \implies x * y > x * z$$

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

$$(1) \quad (x > 0) \implies x * x > 0$$

from: *OrderedField*

$$(2) \quad (x < 0) \implies \dots$$

$$(2.1) \quad -x > 0 \quad \blacksquare \quad x * x = (-x) * (-x) > 0 \quad \blacksquare \quad x * x > 0$$

from: *NegationOnOrder, OrderedField, NegativeMultiplication*

$$(3) \quad (x < 0) \implies x * x > 0$$

$$(4) \quad x \neq 0 \implies (x > 0 \vee x < 0) \implies x * x > 0 \quad \blacksquare \quad x \neq 0 \implies x * x > 0$$

from: *OrderTrichotomy, 1.3*

$$\textcolor{red}{OneIsPositive} := 1 > 0$$

$$(1) \quad 1 \neq 0 \quad \blacksquare \quad 1 = 1 * 1 > 0$$

from: *Field, SquareIsPositive*

$$\textcolor{red}{ReciprocationOnOrder} := (0 < x < y) \implies 0 < 1/y < 1/x$$

$$(1) \quad (0 < x < y) \implies \dots$$

$$(1.1) \quad x * (1/x) = 1 > 0 \quad \blacksquare \quad x * (1/x) > 0$$

from: *Field, OneIsPositive*

$$(1.2) \quad 1/x < 0 \implies x * (1/x) < 0 \wedge x * (1/x) > 0 \implies \perp \quad \blacksquare \quad 1/x > 0$$

from: *NegativeFactorFlipsOrder, 1*

$$(1.3) \quad y * (1/y) = 1 > 0 \quad \blacksquare \quad y * (1/y) > 0$$

from: *Field, OneIsPositive*

$$(1.4) \quad 1/y < 0 \implies y * (1/y) < 0 \wedge y * (1/y) > 0 \implies \perp \quad \blacksquare \quad 1/y > 0$$

from: *NegativeFactorFlipsOrder, 1*

$$(1.5) \quad (1/x) * (1/y) > 0$$

from: *OrderedField*

$$(1.6) \quad 0 < 1/y = ((1/x) * (1/y)) * x < ((1/x) * (1/y)) * y = 1/x$$

from: *OrderedField, 1, 1.4, 1.5*

$$(1.19)$$

$$\textcolor{red}{OrderedFieldQ} := \textcolor{teal}{OrderedField}[\mathbb{Q}, +, *, <] \quad \text{---}$$

$$\textcolor{teal}{Subfield}[K, F, +, *] := \textcolor{teal}{Field}[F, +, *] \wedge K \subset F \wedge \textcolor{teal}{Field}[K, +, *]$$

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

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

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

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

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

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

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

$$(1.1) \quad \forall_{p' \in \alpha} \forall_{q' \in \mathbb{Q}} (q' < p' \implies q' \in \alpha)$$

from: *CutII, 1*

$$(1.2) \quad q < p \implies q \in \alpha \quad \blacksquare \quad q \notin \alpha \implies q \geq p$$

from: 1

$$(1.3) \quad (q \notin \alpha) \implies \dots$$

$$(1.3.1) \quad q \geq p$$

from: 1.2

$$(1.3.2) \quad (q = p) \implies (p \in \alpha \wedge p \notin \alpha) \implies \perp \quad \blacksquare \quad q \neq p$$

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

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

(1)	$(\alpha \in \mathbb{R} \wedge r, s \in \mathbb{Q} \wedge r < s \wedge r \notin \alpha) \implies \dots$	
(1.1)	$\forall_{s' \in \alpha} \forall_{r' \in \mathbb{Q}} (r' < s' \implies r' \in \alpha)$	from: <a href="#">CutII, 1</a>
(1.2)	$s \in \alpha \implies (r \in \mathbb{Q} \implies (r < s \implies r \in \alpha)) \blacksquare s \in \alpha \implies r \in \alpha$	from: 1, 1.1
(1.3)	$r \notin \alpha \implies s \notin \alpha \blacksquare s \notin \alpha$	from: 1, 1.2
(2)	$(\alpha \in \mathbb{R} \wedge r, s \in \mathbb{Q} \wedge r < s \wedge r \notin \alpha) \implies s \notin \alpha$	

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

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

(1)	$(\alpha, \beta \in \mathbb{R}) \implies \dots$	
(1.1)	$\neg(\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta) \implies \dots$	
(1.1.1)	$\alpha \not\subset \beta \wedge \alpha \neq \beta$	from: $<_{\mathbb{R}}$ , 1.1
(1.1.2)	$\exists_{p'} (p' \in \alpha \wedge p' \notin \beta) \blacksquare p := \text{choice}(\{p' : p' \in \alpha \wedge p' \notin \beta\})$	
(1.1.3)	$q \in \beta \implies \dots$	
(1.1.3.1)	$p, q \in \mathbb{Q}$	
(1.1.3.2)	$q < p$	from: <a href="#">CutCorollaryI</a>
(1.1.3.3)	$q \in \alpha$	from: <a href="#">CutII</a>
(1.1.4)	$q \in \beta \implies q \in \alpha$	
(1.1.5)	$\forall_{q \in \beta} (q \in \alpha) \blacksquare \beta \subseteq \alpha$	
(1.1.6)	$\beta \subset \alpha \blacksquare \beta <_{\mathbb{R}} \alpha$	
(1.2)	$\neg(\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta) \implies \beta <_{\mathbb{R}} \alpha$	
(1.3)	$\neg(\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta) \vee (\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta) \blacksquare (\beta <_{\mathbb{R}} \alpha) \vee (\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta)$	
(1.4)	$\alpha = \beta \implies \neg(\alpha <_{\mathbb{R}} \beta \vee \beta <_{\mathbb{R}} \alpha)$	
(1.5)	$\alpha <_{\mathbb{R}} \beta \implies \neg(\alpha = \beta \vee \beta <_{\mathbb{R}} \alpha)$	
(1.6)	$\beta <_{\mathbb{R}} \alpha \implies \neg(\alpha = \beta \vee \alpha <_{\mathbb{R}} \beta)$	
(1.7)	$\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta \vee \alpha <_{\mathbb{R}} \beta$	
(2)	$(\alpha, \beta \in \mathbb{R}) \implies (\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta \vee \alpha <_{\mathbb{R}} \beta)$	
(3)	$\forall_{\alpha, \beta \in \mathbb{R}} (\alpha <_{\mathbb{R}} \beta \vee \alpha = \beta \vee \alpha <_{\mathbb{R}} \beta)$	
(4)	<a href="#">OrderTrichotomy</a> $[\mathbb{R}, <_{\mathbb{R}}]$	

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

(1)	$(\alpha, \beta, \gamma \in \mathbb{R}) \implies \dots$	
(1.1)	$(\alpha <_{\mathbb{R}} \beta \wedge \beta <_{\mathbb{R}} \gamma) \implies \dots$	
(1.1.1)	$\alpha \subset \beta \wedge \beta \subset \gamma$	
(1.1.2)	$\forall_{a \in \alpha} (a \in \beta) \wedge \forall_{b \in \beta} (b \in \gamma)$	
(1.1.3)	$\forall_{a \in \alpha} (\alpha \in \gamma) \blacksquare \alpha \subset \gamma \blacksquare \alpha <_{\mathbb{R}} \gamma$	
(1.2)	$(\alpha <_{\mathbb{R}} \beta \wedge \beta <_{\mathbb{R}} \gamma) \implies \alpha <_{\mathbb{R}} \gamma$	
(2)	$(\alpha, \beta, \gamma \in \mathbb{R}) \implies ((\alpha <_{\mathbb{R}} \beta \wedge \beta <_{\mathbb{R}} \gamma) \implies \alpha <_{\mathbb{R}} \gamma)$	
(3)	$\forall_{\alpha, \beta, \gamma \in \mathbb{R}} ((\alpha <_{\mathbb{R}} \beta \wedge \beta <_{\mathbb{R}} \gamma) \implies \alpha <_{\mathbb{R}} \gamma)$	
(4)	<a href="#">OrderTransitivity</a> $[\mathbb{R}, <_{\mathbb{R}}]$	

**OrderOfR**  $:= \text{Order}[<_{\mathbb{R}}, \mathbb{R}]$

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

(1)	$(\emptyset \neq A \subset \mathbb{R} \wedge \text{BoundedAbove}[A, \mathbb{R}, <_{\mathbb{R}}]) \implies \dots$	from: <a href="#">OrderTrichotomyR</a> , <a href="#">OrderTransitivityR</a> wts:
(1.1)	$\gamma := \{p \in \mathbb{Q} : \exists_{\alpha \in A} (p \in \alpha)\}$	

(1.2)	$A \neq \emptyset \quad \blacksquare \quad \exists_{\alpha}(\alpha \in A) \quad \blacksquare \quad \alpha_0 := \text{choice}(\{\alpha : \alpha \in A\})$
(1.3)	$\alpha_0 \neq \emptyset \quad \blacksquare \quad \exists_a(a \in \alpha_0) \quad \blacksquare \quad a_0 := \text{choice}(\{a : a \in \alpha_0\}) \quad \blacksquare \quad a_0 \in \gamma \quad \blacksquare \quad \gamma \neq \emptyset$
(1.4)	$\text{BoundedAbove}[A, \mathbb{R}, <_{\mathbb{R}}] \quad \blacksquare \quad \exists_{\beta}(\text{UpperBound}[\beta, A, \mathbb{R}, <_{\mathbb{R}}])$
(1.5)	$\beta_0 := \text{choice}(\{\beta : \text{UpperBound}[\beta, A, \mathbb{R}, <_{\mathbb{R}}]\})$
(1.6)	$\text{UpperBound}[\beta_0, A, \mathbb{R}, <_{\mathbb{R}}] \quad \blacksquare \quad \forall_{\alpha \in A}(\alpha \leq_{\mathbb{R}} \beta_0) \quad \blacksquare \quad \forall_{\alpha \in A}(\alpha \subseteq \beta_0) \quad \blacksquare \quad \forall_{\alpha \in A} \forall_{a \in \alpha}(a \in \beta_0)$
(1.7)	$(\alpha \in A \wedge a \in \alpha) \iff a \in \gamma \quad \blacksquare \quad \forall_{a \in \gamma}(a \in \beta_0) \quad \blacksquare \quad \gamma \subseteq \beta_0$
(1.8)	$\beta_0 \subset \mathbb{Q} \quad \blacksquare \quad \gamma \subseteq \beta_0 \subset \mathbb{Q} \quad \blacksquare \quad \gamma \subset \mathbb{Q}$
(1.9)	$\emptyset \neq \gamma \subset \mathbb{Q} \quad \blacksquare \quad \text{CutI}[\gamma]$
(1.10)	$(p \in \gamma \wedge q \in \mathbb{Q} \wedge q < p) \implies \dots$
(1.10.1)	$p \in \gamma \quad \blacksquare \quad \exists_{\alpha \in A}(p \in \alpha) \quad \blacksquare \quad \alpha_1 := \text{choice}(\{\alpha \in A : p \in \alpha\})$
(1.10.2)	$p \in \alpha_1 \wedge q \in \mathbb{Q} \wedge q < p \quad \blacksquare \quad q \in \alpha_1 \quad \blacksquare \quad q \in \gamma$
(1.11)	$(p \in \gamma \wedge q \in \mathbb{Q} \wedge q < p) \implies q \in \gamma \quad \blacksquare \quad \forall_{p \in \gamma} \forall_{q \in \mathbb{Q}}(q < p \implies q \in \gamma) \quad \blacksquare \quad \text{CutII}[\gamma]$
(1.12)	$p \in \gamma \implies \dots$
(1.12.1)	$\exists_{\alpha \in A}(p \in \alpha) \quad \blacksquare \quad \alpha_2 := \text{choice}(\{\alpha \in A : p \in \alpha\})$
(1.12.2)	$\alpha_2 \in \mathbb{R} \quad \blacksquare \quad \text{CutII}[\alpha_2] \quad \blacksquare \quad \exists_{r \in \alpha_2}(p < r) \quad \blacksquare \quad r_0 := \text{choice}(\{r \in \alpha_2 : p < r\})$
(1.12.3)	$r_0 \in \alpha_2 \quad \blacksquare \quad r_0 \in \gamma$
(1.12.4)	$p < r_0 \quad \blacksquare \quad p < r_0 \wedge r_0 \in \gamma \quad \blacksquare \quad \exists_{r \in \gamma}(p < r)$
(1.13)	$p \in \gamma \implies \exists_{r \in \gamma}(p < r) \quad \blacksquare \quad \forall_{p \in \gamma} \exists_{r \in \gamma}(p < r) \quad \blacksquare \quad \text{CutIII}[\gamma]$
(1.14)	$\text{CutI}[\gamma] \wedge \text{CutII}[\gamma] \wedge \text{CutIII}[\gamma] \quad \blacksquare \quad \gamma \in \mathbb{R}$
(1.15)	$\forall_{\alpha \in A}(\alpha \subseteq \gamma) \quad \blacksquare \quad \forall_{\alpha \in A}(\alpha \leq_{\mathbb{R}} \gamma)$
(1.16)	$\forall_{\alpha \in A}(\alpha \leq_{\mathbb{R}} \gamma) \wedge \gamma \in \mathbb{R} \quad \blacksquare \quad \text{UpperBound}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}]$
(1.17)	$\delta <_{\mathbb{R}} \gamma \implies \dots$
(1.17.1)	$\delta \subset \gamma \quad \blacksquare \quad \exists_s(s \in \gamma \wedge s \notin \delta) \quad \blacksquare \quad s_0 := \text{choice}(\{s \in \mathbb{Q} : s \in \gamma \wedge s \notin \delta\})$
(1.17.2)	$s_0 \in \gamma \quad \blacksquare \quad \exists_{\alpha \in A}(s_0 \in \alpha) \quad \blacksquare \quad \alpha_3 := \text{choice}(\{\alpha \in A : s_0 \in \alpha\})$
(1.17.3)	$s_0 \in \alpha_3 \wedge s_0 \notin \delta \quad \blacksquare \quad \exists_{s \in \mathbb{Q}}(s \in \alpha_3 \wedge s \notin \delta)$
(1.17.4)	$\delta \geq_{\mathbb{R}} \alpha_3 \implies \dots$
(1.17.4.1)	$\alpha_3 \subseteq \delta \quad \blacksquare \quad \forall_{s \in \mathbb{Q}}(s \in \alpha_3 \implies s \in \delta) \quad \blacksquare \quad \neg \exists_{s \in \mathbb{Q}}(s \in \alpha_3 \wedge s \notin \delta)$
(1.17.4.2)	$\neg \exists_{s \in \mathbb{Q}}(s \in \alpha_3 \wedge s \notin \delta) \wedge \exists_{s \in \mathbb{Q}}(s \in \alpha_3 \wedge s \notin \delta) \quad \blacksquare \quad \perp$
(1.17.5)	$\delta \geq_{\mathbb{R}} \alpha_3 \implies \perp \quad \blacksquare \quad \delta <_{\mathbb{R}} \alpha_3 \quad \blacksquare \quad \exists_{\alpha \in A}(\delta <_{\mathbb{R}} \alpha) \quad \blacksquare \quad \exists_{\alpha \in A}(\neg(\alpha \leq_{\mathbb{R}} \delta))$
(1.17.6)	$\neg \forall_{\alpha \in A}(\alpha \leq_{\mathbb{R}} \delta) \quad \blacksquare \quad \neg \text{UpperBound}[\delta, A, \mathbb{R}, <_{\mathbb{R}}]$
(1.18)	$\delta <_{\mathbb{R}} \gamma \implies \neg \text{UpperBound}[\delta, A, \mathbb{R}, <_{\mathbb{R}}] \quad \blacksquare \quad \forall_{\delta}(\delta <_{\mathbb{R}} \gamma \implies \neg \text{UpperBound}[\delta, A, \mathbb{R}, <_{\mathbb{R}}])$
(1.19)	$\text{UpperBound}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}] \wedge \forall_{\delta}(\delta <_{\mathbb{R}} \gamma \implies \neg \text{UpperBound}[\delta, A, \mathbb{R}, <_{\mathbb{R}}])$
(1.20)	$\text{LUB}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}] \quad \blacksquare \quad \exists_{\gamma \in S}(\text{LUB}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}])$
(2)	$(\emptyset \neq A \subset \mathbb{R} \wedge \text{BoundedAbove}[A, \mathbb{R}, <_{\mathbb{R}}]) \implies \exists_{\gamma \in S}(\text{LUB}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}])$
(3)	$\forall_A \left( (\emptyset \neq A \subset \mathbb{R} \wedge \text{BoundedAbove}[A, \mathbb{R}, <_{\mathbb{R}}]) \implies \exists_{\gamma \in S}(\text{LUB}[\gamma, A, \mathbb{R}, <_{\mathbb{R}}]) \right) \quad \blacksquare \quad \text{LUBProperty}[\mathbb{R}, <_{\mathbb{R}}]$

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

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

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

(1)	$-1 \in 0_{\mathbb{R}} \wedge 1 \notin 0_{\mathbb{R}} \quad \blacksquare \quad \emptyset \neq 0_{\mathbb{R}} \subseteq \mathbb{Q} \quad \blacksquare \quad \text{CutI}[0_{\mathbb{R}}]$
(2)	$(x \in 0_{\mathbb{R}} \wedge y \in \mathbb{Q} \wedge y < x) \implies y < x < 0 \implies y < 0 \implies y \in 0_{\mathbb{R}} \quad \blacksquare \quad \forall_{x \in 0_{\mathbb{R}}} \forall_{y \in \mathbb{Q}}(y_0 < x \implies y \in 0_{\mathbb{R}}) \quad \blacksquare \quad \text{CutII}[0_{\mathbb{R}}]$
(3)	$y := x/2 \quad \blacksquare \quad (x \in 0_{\mathbb{R}}) \implies (x < y < 0) \implies \exists_{y \in 0_{\mathbb{R}}}(x < y) \quad \blacksquare \quad \forall_{x \in 0_{\mathbb{R}}} \exists_{y \in 0_{\mathbb{R}}}(x < y) \quad \blacksquare \quad \text{CutIII}[0_{\mathbb{R}}]$
(4)	$\text{CutI}[0_{\mathbb{R}}] \wedge \text{CutII}[0_{\mathbb{R}}] \wedge \text{CutIII}[0_{\mathbb{R}}] \quad \blacksquare \quad 0_{\mathbb{R}} \in \mathbb{R}$

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

(1)	$(\alpha, \beta \in \mathbb{R}) \implies \dots$
(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)  $\emptyset \neq \alpha +_{\mathbb{R}} \beta \subset \mathbb{Q} \blacksquare \textcolor{blue}{CutI}[\alpha +_{\mathbb{R}} \beta]$
- (1.7)  $(p \in \alpha +_{\mathbb{R}} \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies \dots$
- (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)  $(p \in \alpha +_{\mathbb{R}} \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies q \in \alpha +_{\mathbb{R}} \beta \blacksquare \forall_{p \in \alpha +_{\mathbb{R}} \beta} \forall_{q \in \mathbb{Q}}(q < p \implies q \in \alpha +_{\mathbb{R}} \beta) \blacksquare \textcolor{blue}{CutII}[\alpha +_{\mathbb{R}} \beta]$
- (1.9)  $p \in \alpha \implies \dots$
- (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)  $p \in \alpha \implies \exists_{r \in \alpha +_{\mathbb{R}} \beta}(p < r) \blacksquare \forall_{p \in \alpha +_{\mathbb{R}} \beta} \exists_{r \in \alpha +_{\mathbb{R}} \beta}(p < r) \blacksquare \textcolor{blue}{CutIII}[\alpha +_{\mathbb{R}} \beta]$
- (1.11)  $\textcolor{blue}{CutI}[\alpha +_{\mathbb{R}} \beta] \wedge \textcolor{blue}{CutII}[\alpha +_{\mathbb{R}} \beta] \wedge \textcolor{blue}{CutIII}[\alpha +_{\mathbb{R}} \beta] \blacksquare \alpha +_{\mathbb{R}} \beta \in \mathbb{R}$
- (2)  $(\alpha, \beta \in \mathbb{R}) \implies ((\alpha +_{\mathbb{R}} \beta) \in \mathbb{R})$

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

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

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

- (1)  $(\alpha, \beta, \gamma \in \mathbb{R}) \implies \dots$
- (1.1)  $(\alpha +_{\mathbb{R}} \beta) +_{\mathbb{R}} \gamma = \{(a + b) + c : a \in \alpha \wedge b \in \beta \wedge c \in \gamma\} = \dots$
- (1.2)  $\{a + (b + c) : a \in \alpha \wedge b \in \beta \wedge c \in \gamma\} = \alpha +_{\mathbb{R}} (\beta +_{\mathbb{R}} \gamma)$
- (2)  $(\alpha, \beta, \gamma \in \mathbb{R}) \implies (\alpha +_{\mathbb{R}} \beta) +_{\mathbb{R}} \gamma = \alpha +_{\mathbb{R}} (\beta +_{\mathbb{R}} \gamma)$

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

- (1)  $\alpha \in \mathbb{R} \implies \dots$
- (1.1)  $(r \in \alpha \wedge s \in 0_{\mathbb{R}}) \implies \dots$
- (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)  $p \in \alpha \implies \dots$
- (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)  $\alpha \in \mathbb{R} \implies 0_{\mathbb{R}} +_{\mathbb{R}} \alpha = \alpha$

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

- (1)  $\alpha \in \mathbb{R} \implies \dots$
- (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)  $r > 0 \implies \dots$
- (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)  $\emptyset \neq \beta \subset \mathbb{Q} \blacksquare \textcolor{blue}{CutI}[\beta]$

(1.8)	$(p \in \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies \dots$	
(1.8.1)	$p \in \beta \blacksquare \exists_{r>0}(-p-r \notin \alpha) \blacksquare r_0 := \text{choice}(\{r > 0 : -p-r \notin \alpha\})$	
(1.8.2)	$q < p \blacksquare -p-r < -q-r$	
(1.8.3)	$-q-r \notin \alpha \blacksquare q \in \beta$	
(1.9)	$(p \in \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies q \in \beta \blacksquare \forall_{p \in \beta} \forall_{q \in \mathbb{Q}}(q < p \implies q \in \beta) \blacksquare \text{CutII}[\beta]$	
(1.10)	$p \in \beta \implies \dots$	
(1.10.1)	$p \in \beta \blacksquare \exists_{r>0}(-p-r \notin \alpha) \blacksquare r_1 := \text{choice}(\{r > 0 : -p-r \notin \alpha\})$	
(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)	$p \in \beta \implies \exists_{t \in \beta}(p < t) \blacksquare \forall_{p \in \beta} \exists_{t \in \beta}(p < t) \blacksquare \text{CutIII}[\beta]$	
(1.12)	$\text{CutI}[\beta] \wedge \text{CutII}[\beta] \wedge \text{CutIII}[\beta] \blacksquare \beta \in \mathbb{R}$	
(1.13)	$(r \in \alpha \wedge s \in \beta) \implies \dots$	
(1.13.1)	$s \in \beta \blacksquare \exists_{t>0}(-s-t \notin \alpha) \blacksquare t_1 := \text{choice}(\{t > 0 : -s-t \notin \alpha\}) \blacksquare -s - t_1 < -s$	
(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)	$v \in 0_{\mathbb{R}} \implies \dots$	
(1.15.1)	$v < 0 \blacksquare w_0 := -v/2 \blacksquare w > 0$	
(1.15.2)	$\exists_{n \in \mathbb{Z}}(nw_0 \in \alpha \wedge (n+1)w_0 \notin \alpha) \blacksquare n_0 := \text{choice}(\{n \in \mathbb{Z} : nw_0 \in \alpha \wedge (n+1)w_0 \notin \alpha\})$	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)	$\alpha \in \mathbb{R} \implies \exists_{-\alpha \in \mathbb{R}}(\alpha +_{\mathbb{R}} (-\alpha) = 0_{\mathbb{R}})$	

$*_{\mathbb{R}}[\alpha, \beta] := \quad \quad \quad \text{---}$   
 $1_{\mathbb{R}} := \{x \in \mathbb{Q} : x < 1\}$

$11s\text{Nor}0 := 0_{\mathbb{R}} \neq 1_{\mathbb{R}} \quad \quad \quad \text{---}$   
 $11nR := 1_{\mathbb{R}} \in \mathbb{R} \quad \quad \quad \text{---}$

$\text{Field Multiplication Closure Of } \mathbb{R} := (\alpha, \beta \in \mathbb{R}) \implies (\alpha *_{\mathbb{R}} \beta) \in \mathbb{R} \quad \quad \quad \text{---}$   
 $\text{Field Multiplication Commutativity Of } \mathbb{R} := (\alpha, \beta \in \mathbb{R}) \implies (\alpha *_{\mathbb{R}} \beta = \beta *_{\mathbb{R}} \alpha) \quad \quad \quad \text{---}$   
 $\text{Field Multiplication Associativity Of } \mathbb{R} := (\alpha, \beta, \gamma \in \mathbb{R}) \implies ((\alpha *_{\mathbb{R}} \beta) *_{\mathbb{R}} \gamma = \alpha *_{\mathbb{R}} (\beta *_{\mathbb{R}} \gamma)) \quad \quad \quad \text{---}$   
 $\text{Field Multiplication Identity Of } \mathbb{R} := (\alpha \in \mathbb{R}) \implies 1_{\mathbb{R}} *_{\mathbb{R}} \alpha = \alpha \quad \quad \quad \text{---}$   
 $\text{Field Multiplication Inverse Of } \mathbb{R} := (\alpha \in \mathbb{R}) \implies \exists_{1/\alpha \in \mathbb{R}}(\alpha *_{\mathbb{R}} (1/\alpha) = 1_{\mathbb{R}}) \quad \quad \quad \text{---}$

$\text{Field Distributativity Of } \mathbb{R} := (\alpha, \beta, \gamma \in \mathbb{R}) \implies \gamma *_{\mathbb{R}} (\alpha +_{\mathbb{R}} \beta) = \gamma *_{\mathbb{R}} \alpha + \gamma *_{\mathbb{R}} \beta \quad \quad \quad \text{---}$

$\text{Field With } \mathbb{R} := \text{Field}[\mathbb{R}, +_{\mathbb{R}}, *_{\mathbb{R}}] \quad \quad \quad \text{---}$   
 $\text{Ordered Field With } \mathbb{R} := \text{OrderedField}[\mathbb{R}, +_{\mathbb{R}}, *_{\mathbb{R}}, <_{\mathbb{R}}] \quad \quad \quad \text{---}$

$\mathbb{Q}_{\mathbb{R}} := \{\{r \in \mathbb{Q} : r < q\} : q \in \mathbb{Q}\}$   
 $\text{QROrderedSubfieldOf } \mathbb{R} := \text{OrderedSubfield}[\mathbb{Q}_{\mathbb{R}}, \mathbb{R}, +_{\mathbb{R}}, *_{\mathbb{R}}, <_{\mathbb{R}}] \quad \quad \quad \text{---}$   
 $\text{QIsomorphicToQR} := \mathbb{Q}_{\mathbb{R}} \simeq \mathbb{Q} \quad \quad \quad \text{---}$   
 $\text{Completeness Of } \mathbb{R} := \exists_{\mathbb{R}}(\text{LUBProperty}[\mathbb{R}, <_{\mathbb{R}}] \wedge \text{OrderedSubfield}[\mathbb{Q}, \mathbb{R}, +_{\mathbb{R}}, *_{\mathbb{R}}, <_{\mathbb{R}}]) \quad \quad \quad \text{---}$

(1.20)  
 $\text{ArchimedeanPropertyOf } \mathbb{R} := \forall_{x,y \in \mathbb{R}}(x > 0 \implies \exists_{n \in \mathbb{N}^+}(nx > y))$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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)

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

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

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

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

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

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

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

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

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

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

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

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

$$(1.4) \quad 1 = (1+x)/(1+x) > x/(1+x) = t_0 \quad \blacksquare \quad 1 > t_0$$

$$(1.5) \quad (t_0 > 0) \wedge (1 > t_0) \quad \blacksquare \quad 0 < t_0 < 1$$

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

$$(1.7) \quad 0 < x \quad \blacksquare \quad x > x/(1+x) = t_0 \quad \blacksquare \quad x > t_0$$

$$(1.8) \quad (t_0^n \leq t_0) \wedge (x > t_0) \quad \blacksquare \quad t_0^n < x$$

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

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

$$(1.11) \quad x > 0 \quad \blacksquare \quad t_1 > 1+x > 1 \quad \blacksquare \quad t_1 > 1 \quad \blacksquare \quad t_1^n \geq t_1$$

$$(1.12) \quad (t_1^n \geq t_1) \wedge (t_1 > 1+x) \wedge (1 > 0) \quad \blacksquare \quad t_1^n \geq t_1 > 1+x > x \quad \blacksquare \quad t_1^n > x$$

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

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

$$(1.15) \quad t \in E \implies \dots$$

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

$$(1.15.2) \quad (t_1^n > x) \wedge (t^n < x) \quad \blacksquare \quad t^n < x < t_1^n \quad \blacksquare \quad t < t_1$$

$$(1.16) \quad t \in E \implies t < t_1 \quad \blacksquare \quad \forall_{t \in E} (t \leq t_1) \quad \blacksquare \quad \text{Upper Bound}[t_1, E, \mathbb{R}, <] \quad \blacksquare \quad \text{Bounded Above}[E, \mathbb{R}, <]$$

$$(1.17) \quad \text{Completeness Of } \mathbb{R} \quad \blacksquare \quad \text{LUB Property}[\mathbb{R}, <]$$

$$(1.18) \quad (\text{LUB Property}[\mathbb{R}, <]) \wedge (\emptyset \neq E \subset \mathbb{R}) \wedge (\text{Bounded Above}[E, \mathbb{R}, <]) \quad \blacksquare \quad \exists_{y \in \mathbb{R}} (\text{LUB}[y, E, \mathbb{R}, <]) \quad \dots$$

$$(1.19) \quad \dots y_0 := \text{choice}(\{y \in \mathbb{R} : \text{LUB}[y, E, \mathbb{R}, <]\}) \quad \blacksquare \quad \text{LUB}[y_0, E, \mathbb{R}, <]$$

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

$$(1.21) \quad y_0^n < x \implies \dots$$

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

$$(1.21.2) \quad y_0^n < x \quad \blacksquare \quad 0 < x - y_0^n$$

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

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

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

$$(1.21.6) \quad \text{QDense In } \mathbb{R} \wedge (0, \min(1, k_0)) \in \mathbb{R} \wedge (0 < \min(1, k_0)) \quad \blacksquare \quad \exists_{h \in \mathbb{Q}} (0 < h < \min(1, k_0)) \quad \dots$$

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

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

$$(1.21.9) \quad \text{Root Lemma} \wedge (0 < y_0 < y_0 + h_0) \quad \blacksquare \quad (y_0 + h_0)^n - y_0^n < h_0 n(y_0 + h_0)^{n-1}$$

$$(1.21.10) \quad h_0 < 1 \quad \blacksquare \quad h_0 n(y_0 + h_0)^{n-1} < h_0 n(y_0 + 1)^{n-1}$$

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

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

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

$$(1.21.14) \quad (y_0 + h_0)^n - y_0^n < x - y_0^n \quad \blacksquare \quad (y_0 + h_0)^n < x$$

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

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

(1.21.17)	$((y_0 + h_0)^n \in E) \wedge (y_0 < y_0 + h_0) \blacksquare \exists_{e \in E} (y_0 < e)$
(1.21.18)	$\textcolor{blue}{LUB}[y_0, E, \mathbb{R}, <] \blacksquare \textcolor{blue}{UpperBound}[y_0, E, \mathbb{R}, <] \blacksquare \forall_{e \in E} (e \leq y_0) \blacksquare \neg \exists_{e \in E} (e > y_0)$
(1.21.19)	$(\exists_{e \in E} (e > y_0)) \wedge (\neg \exists_{e \in E} (e > y_0)) \blacksquare \perp$
(1.22)	$y_0^n < x \implies \perp \blacksquare y_0^n \geq x$
(1.23)	$y_0^n > x \implies \dots$
(1.23.1)	$k_1 := \frac{y_0^n - x}{ny_0^{n-1}} \blacksquare (k_1 \in \mathbb{R}) \wedge (k_1 ny_0^{n-1} = y_0^n - x)$
(1.23.2)	$(0 < x) \wedge (0 < n \in \mathbb{Z}) \blacksquare y_0^n - x < y_0^n \leq ny_0^n \blacksquare y_0^n - x < ny_0^n$
(1.23.3)	$y_0^n - x < ny_0^n \blacksquare k_1 = \frac{y_0^n - x}{ny_0^{n-1}} < \frac{ny_0^n}{ny_0^{n-1}} = y_0 \blacksquare k_1 < y_0$
(1.23.4)	$y_0^n > x \blacksquare 0 < y_0^n - x$
(1.23.5)	$(n > 0) \wedge (y_0 > 0) \blacksquare 0 < ny_0^{n-1}$
(1.23.6)	$(0 < y_0^n - x) \wedge 0 < (ny_0^{n-1}) \blacksquare 0 < \frac{y_0^n - x}{ny_0^{n-1}} = k_1 \blacksquare 0 < k_1$
(1.23.7)	$(k_1 < y_0) \wedge (0 < k_1) \blacksquare (0 < k_1 < y_0) \wedge (0 < y_0 - k_1 < y_0)$
(1.23.8)	$t \geq y_0 - k_1 \implies \dots$
(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)	$\textcolor{blue}{RootLemma} \wedge (0 < y_0 - k_1 < y_0) \blacksquare y_0^n - (y_0 - k_1)^n < k_1 ny_0^{n-1}$
(1.23.8.3)	$(y_0^n - t^n \leq y_0^n - (y_0 - k_1)^n) \wedge (y_0^n - (y_0 - k_1)^n < k_1 ny_0^{n-1}) \blacksquare y_0^n - t^n < k_1 ny_0^{n-1}$
(1.23.8.4)	$(k_1 ny_0^{n-1} = y_0^n - x) \wedge (y_0^n - t^n < k_1 ny_0^{n-1}) \blacksquare y_0^n - t^n < y_0^n - x \blacksquare -t^n < -x \blacksquare t^n > x$
(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)	$t \geq y_0 - k_1 \implies t \notin E \blacksquare t \in E \implies t < y_0 - k_1 \blacksquare \forall_{t \in E} (t \leq y_0 - k_1) \blacksquare \textcolor{blue}{UpperBound}[y_0 - k_1, E, \mathbb{R}, <]$
(1.23.10)	$(\textcolor{blue}{LUB}[y_0, E, \mathbb{R}, <] \wedge (y_0 - k_1 < y_0)) \blacksquare \neg \textcolor{blue}{UpperBound}[y_0 - k_1, E, \mathbb{R}, <]$
(1.23.11)	$(\textcolor{blue}{UpperBound}[y_0 - k_1, E, \mathbb{R}, <]) \wedge (\neg \textcolor{blue}{UpperBound}[y_0 - k_1, E, \mathbb{R}, <]) \blacksquare \perp$
(1.24)	$y_0^n > x \implies \perp \blacksquare y_0^n \leq x$
(1.25)	$\textcolor{blue}{Order}[\mathbb{R}, <] \blacksquare \textcolor{blue}{OrderTrichotomy}[\mathbb{R}, <]$
(1.26)	$(\textcolor{blue}{OrderTrichotomy}[\mathbb{R}, <]) \wedge (y_0^n \geq x) \wedge (y_0^n \leq x) \blacksquare y_0^n = x$
(1.27)	$(y_0^n = x) \wedge (y_0 \in \mathbb{R}) \blacksquare \exists_{y \in \mathbb{R}} (y^n = x)$
(1.28)	$y_1, y_2 := \textit{choice}(\{y \in \mathbb{R} : y^n = x\})$
(1.29)	$y_1 \neq y_2 \implies \dots$
(1.29.1)	$(\textcolor{blue}{OrderTrichotomy}[\mathbb{R}, <]) \wedge (y_1 \neq y_2) \blacksquare (y_1 < y_2) \vee (y_2 < y_1) \dots$
(1.29.2)	$\dots (x = y_1^n < y_2^n = x) \vee (x = y_2^n < y_1^n = x) \blacksquare (x < x) \vee (x > x) \blacksquare \perp \vee \perp \blacksquare \perp$
(1.30)	$y_1 \neq y_2 \implies \perp \blacksquare y_1 = y_2 \blacksquare \forall_{a,b \in \mathbb{R}} ((a^n = x \wedge b^n = x) \implies a = b)$
(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)	$(0 < x \in \mathbb{R} \wedge 0 < n \in \mathbb{Z}) \implies \exists!_{y \in \mathbb{R}} (y^n = x) \blacksquare \forall_{0 < x \in \mathbb{R}} \forall_{0 < n \in \mathbb{Z}} \exists!_{0 < y \in \mathbb{R}} (y_0^n = x)$

$$\textcolor{red}{RootExistenceInRCorollary} := \forall_{0 < a \in \mathbb{R}} \forall_{0 < b \in \mathbb{R}} \forall_{0 < n \in \mathbb{Z}} \left( (ab)^{1/n} = a^{1/n} b^{1/n} \right) \quad \text{---}$$

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

$$\mathbb{C} := \{\langle a, b \rangle \in \mathbb{R} \times \mathbb{R}\}$$

$$+_C[\langle a, b \rangle, \langle c, d \rangle] := \langle a +_{\mathbb{R}} c, b +_{\mathbb{R}} d \rangle$$

$$*_C[\langle a, b \rangle, \langle c, d \rangle] := \langle a *_R c - b *_R d, a *_R d + b *_R c \rangle$$

$$\textcolor{red}{FieldC} := \textcolor{blue}{Field}[\mathbb{C}, +_C, *_C] \quad \text{---}$$

$$\textcolor{red}{RSubfieldC} := \textcolor{blue}{Subfield}[\mathbb{R}, \mathbb{C}, +, *] \quad \text{---}$$

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

$$\textcolor{red}{iProperty} := i^2 = -1 \quad \text{---}$$

$$\textcolor{red}{CProperty} := (a, b \in \mathbb{R}) \implies (\langle a, b \rangle = a + bi) \quad \text{---}$$



# Chapter 2

## Abstract Algebra

### 2.1 Functions

$$Rel[r, X] := (X \neq \emptyset) \wedge (r \subseteq X)$$

$$Func[f, X, Y] := (Rel[f, X \times Y]) \wedge \left( \forall_{x \in X} \exists!_{y \in Y} (\langle x, y \rangle \in f) \right)$$

$$Comp[g \circ f, f, g, X, Y, Z] := (Func[f, X, Y]) \wedge (Func[g, Y, Z]) \wedge \left( g \circ f = \{ \langle x, g(f(x)) \rangle \in X \times Z \mid x \in X \} \right)$$

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

---

(1) TODO

---

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

---

(1) TODO

---

$$Domain[dom(f), f, X, Y] := (Func[f, X, Y]) \wedge (dom(f) = X)$$

$$Codomain[cod(f), f, X, Y] := (Func[f, X, Y]) \wedge (cod(f) = Y)$$

$$Image[im(A), A, f, X, Y] := (Func[f, X, Y]) \wedge (A \subseteq X) \wedge (im(A) = \{ f(a) \in Y \mid a \in A \})$$

$$Preimage[pim(B), B, f, X, Y] := (Func[f, X, Y]) \wedge (B \subseteq Y) \wedge (pim(B) = \{ a \in X \mid f(a) \in B \})$$

$$Range[rng(f), f, X, Y] := (Func[f, X, Y]) \wedge (Image[rng(f), dom(f), f, X, Y])$$

$$Inj[f, X, Y] := (Func[f, X, Y]) \wedge \left( \forall_{x_1, x_2 \in X} \left( (f(x_1) = f(x_2)) \implies (x_1 = x_2) \right) \right)$$

$$Surj[f, X, Y] := (Func[f, X, Y]) \wedge \left( \forall_{y \in Y} \exists_{x \in X} (y = f(x)) \right)$$

$$Bij[f, X, Y] := (Inj[f, X, Y]) \wedge (Surj[f, X, Y])$$

$$Inv[f^{-1}, f, X, Y] := (Func[f, X, Y]) \wedge (Func[f^{-1}, Y, X]) \wedge (f \circ f^{-1} = I_Y) \wedge (f^{-1} \circ f = I_X)$$

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

---

(1) TODO

---

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

---

(1) TODO

---

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

---

(1) TODO

---

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

---

(1) TODO

---

## 2.2 Divisibility, Equivalence Relations, Partitions

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

---

(1) TODO

---

$$\text{Divides}[a, b] := (a, b \in \mathbb{Z}) \wedge (\exists_{c \in \mathbb{Z}} (b = ac))$$

$$\text{ComDiv}[a, b, c] := (\text{Divides}[a, b]) \wedge (\text{Divides}[a, c])$$

$$\text{GCD}[a, b, c] := (\text{ComDiv}[a, b, c]) \wedge \left( \forall_{d \in \mathbb{Z}} \left( ((\text{Divides}[d, b]) \wedge (\text{Divides}[d, c])) \implies (\text{Divides}[d, a]) \right) \right)$$

$$\text{RelPrime}[a, b] := \text{GCD}[1, a, b]$$

$$\text{CongRel}[a, b, n] := \text{Divides}[n, a - b]$$

$$\text{Partition}[\mathcal{P}, S] := (\forall_{P \in \mathcal{P}} (P \neq \emptyset)) \wedge \left( S = \bigcup_{P \in \mathcal{P}} (P) \right) \wedge \left( \forall_{P_1, P_2 \in \mathcal{P}} ((P_1 \neq P_2) \implies (P_1 \cap P_2 = \emptyset)) \right)$$

$$\text{EqRel}[\sim, S] := (\text{Rel}[\sim, S]) \wedge (\forall_{a \in S} (a \sim a)) \wedge \left( \forall_{a, b \in S} ((a \sim b) \implies (b \sim a)) \right) \wedge \left( \forall_{a, b, c \in S} (((a \sim b) \wedge (b \sim c)) \implies (a \sim c)) \right)$$

$$\text{EqClass}[[s], s, \sim, S] := (\text{Rel}[\sim, S]) \wedge (s \in S) \wedge ([s] = \{x \in S \mid x \sim s\})$$

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

---

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

---

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

---

(1) TODO :  $\text{Partition}[\text{EqClass}_1, \text{EqClass}_2, \dots]$

---

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

---

(1) TODO

---

## 2.3 Groups

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

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

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

---

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

---

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

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

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

---

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

---

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

---

(3.1) TODO

---

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

---

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

---

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

---

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

---



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

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

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

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

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

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

$$OrderEl[o(G), G, *] := (Group[G, *]) \wedge (o(G) = |G|)$$

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

$$OrderEl[o(g), g, G, *] := (Group[G, *]) \wedge \left( (\exists_n (gWitness[n, g, G, *])) \implies (o(g) = n) \right) \wedge \left( (\neg \exists_n (gWitness[n, g, G, *])) \implies (o(g) = \infty) \right)$$

## 2.4 Subgroups

$$Subgroup[H, G, *] := (Group[G, *]) \wedge (H \subseteq G) \wedge (Group[H, *])$$

$$TrivSubgroup[H, G, *] := (H = \{e\}) \vee (H = G)$$

$$PropSubgroup[H, G, *] := (Subgroup[H, G, *]) \wedge (\neg TrivSubgroup[H, G, *])$$

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

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

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

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

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

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

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

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

$$(2.6) \quad Group[H, *]$$

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

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

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

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

$$(1) \quad \text{TODO}$$

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

$$(1) \quad Group[G, *]$$

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

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

- 
- (4)  $\emptyset \neq H_1 \cap H_2 \subseteq G$
- 
- (5)  $(a, b \in H_1 \cap H_2) \implies \dots$
- 
- (5.1)  $a, b \in H_1 \blacksquare a * b \in H_1$
- 
- (5.2)  $a, b \in H_2 \blacksquare a * b \in H_2$
- 
- (5.3)  $a * b \in H_1 \cap H_2$
- 
- (6)  $(a, b \in H_1 \cap H_2) \implies (a * b \in H_1 \cap H_2) \blacksquare \text{Function}[* , H_1 \cap H_2, H_1 \cap H_2]$
- 
- (7)  $(a \in H_1 \cap H_2) \implies \dots$
- 
- (7.1)  $(a^{-1} \in H_1) \wedge (a^{-1} \in H_2) \blacksquare a^{-1} \in H_1 \cap H_2$
- 
- (8)  $(a \in H_1 \cap H_2) \implies (a^{-1} \in H_1 \cap H_2) \blacksquare \forall_{a \in H_1 \cap H_2} \exists_{a^{-1} \in H_1 \cap H_2} (a * a^{-1} = e = a^{-1} * a)$
- 
- (9)  $(\text{SubgroupEquiv}) \wedge (\text{Group}[G, *]) \wedge (\emptyset \neq H_1 \cap H_2 \subseteq G) \wedge (\text{Function}[* , H_1 \cap H_2, H_1 \cap H_2]) \wedge \dots$
- 
- (10)  $\dots \left( \forall_{a \in H_1 \cap H_2} \exists_{a^{-1} \in H_1 \cap H_2} (a * a^{-1} = e = a^{-1} * a) \right) \blacksquare \text{Subgroup}[H_1 \cap H_2, G, *]$
- 

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

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

- 
- (1)  $e * g = g * e \blacksquare e \in C(g) \blacksquare C(g) \neq \emptyset$
- 
- (2)  $C(g) \subseteq G \blacksquare \emptyset \neq C(g) \subseteq G$
- 
- (3)  $(a, b \in C(g)) \implies \dots$
- 
- (3.1)  $(a * g = g * a) \wedge (b * g = g * b)$
- 
- (3.2)  $(a * b) * g = a * (b * g) = a * (g * b) = (a * g) * b = (g * a) * b = g * (a * b) \blacksquare a * b \in C(g)$
- 
- (4)  $(a, b \in C(g)) \implies (a * b \in C(g)) \blacksquare \forall_{a, b \in C(g)} (a * b \in C(g))$
- 
- (5)  $(a \in C(g)) \implies \dots$
- 
- (5.1)  $a * g = g * a$
- 
- (5.2)  $a^{-1} * (a * g) * a^{-1} = a^{-1} * (g * a) * a^{-1} \blacksquare g * a^{-1} = a^{-1} * g \blacksquare a^{-1} \in C(g)$
- 
- (6)  $(a \in C(g)) \implies (a^{-1} \in C(g)) \blacksquare \forall_{a \in C(g)} (a^{-1} \in C(g))$
- 
- (7)  $(\text{SubgroupEquiv}) \wedge (\emptyset \neq C(g) \subseteq G) \wedge \left( \forall_{a, b \in C(g)} (a * b \in C(g)) \right) \wedge \left( \forall_{a \in C(g)} (a^{-1} \in C(g)) \right) \blacksquare \text{Subgroup}[C(g), G, *]$
- 

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

$$\text{SubgroupCenter} := \forall_G \left( (\text{Center}[Z(G), G, *]) \implies (\text{Subgroup}[Z(G), G, *]) \right)$$

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

## 2.5 Special Groups

### 2.5.1 Cyclic Group

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

$$\text{Generator}[g, G, *] := \text{CyclicSubgroup}[G, g, G, *]$$

$$\text{CyclicGroup}[G, *] := \exists_{g \in G} (\text{Generator}[g, G, *])$$

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

- 
- (1)  $\exists_{g \in G} (\text{Generator}[g, G, *])$
- 
- (2)  $H \subseteq G \blacksquare \exists_{m \in \mathbb{Z}^+} \left( (g^m \in H) \wedge \left( \forall_{k \in \mathbb{Z}^+} ((k < m) \implies (g^k \notin H)) \right) \right)$
- 
- (3)  $(b \in H) \implies \dots$
- 
- (3.1)  $H \subseteq G \blacksquare \exists_{n \in \mathbb{Z}^+} (b = g^n)$
- 
- (3.2)  $(\text{DivisionAlgorithm}) \wedge (n \in \mathbb{Z}) \wedge (m \in \mathbb{Z}^+) \blacksquare \exists!_{q, r \in \mathbb{Z}} ((n = mq + r) \wedge (0 \leq r < m))$
-

---

(3.3)	$g^n = g^{mq+r} = g^{mq} * g^r \quad \blacksquare \quad g^r = (g^{mq})^{-1} * g^n$
(3.4)	$g^n, g^m \in H \quad \blacksquare \quad g^n, (g^{mq})^{-1} \in H \quad \blacksquare \quad g^r = g^{mq})^{-1} * g^n \in H \quad \blacksquare \quad g^r \in H$
(3.5)	$(g^r \in H) \wedge (0 \leq r < m) \wedge \left( \bigvee_{k \in \mathbb{Z}^+} ((k < m) \implies (g^k \notin H)) \right) \quad \blacksquare \quad r = 0$
(3.6)	$(r = 0) \wedge (g^n = g^{mq+r}) \wedge (b = g^n) \quad \blacksquare \quad b = g^n = g^{mq} \quad \blacksquare \quad b \in < g^m >$
(4)	$(b \in H) \implies (b \in < g^m >) \quad \blacksquare \quad H \subseteq < g^m >$
(5)	$(b \in < g^m >) \implies \dots$
(5.1)	$\exists_{k \in \mathbb{Z}} (b = (g^m)^k)$
(5.2)	$(Group[H, G, *]) \wedge (g^m \in H) \quad \blacksquare \quad (g^m * g^m \in H) \wedge ((g^m)^{-1} \in H)$
(5.3)	<i>Induction</i> $\blacksquare b = (g^m)^k \in H \quad \blacksquare b \in H$
(6)	$(b \in < g^m >) \implies (b \in H) \quad \blacksquare \quad < g^m > \subseteq H$
(7)	$(H \subseteq < g^m >) \wedge (< g^m > \subseteq H) \quad \blacksquare \quad H = < g^m > \quad \blacksquare \quad Generator[g^m, H, *] \quad \blacksquare \quad \exists_{h \in G} (Generator[h, G, *]) \quad \blacksquare \quad CyclicGroup[H, *]$

---

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

- 
- |     |                                                                                                                           |
|-----|---------------------------------------------------------------------------------------------------------------------------|
| (1) | $(s \equiv t(mod\ n)) \iff (Divides[n, s - t]) \iff (\exists_{k \in \mathbb{N}} (s - t = kn)) \iff \dots$                 |
| (2) | $\dots (\exists_{k \in \mathbb{N}} (s = kn + t)) \iff (g^s = g^{kn+t} = g^{kn} * g^t = e^k * g^t = g^t) \iff (g^s = g^t)$ |
- 

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

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

## 2.5.2 Symmetric and Alternating Groups

$$SymmetricGroup[S_n, n] := S_n = \{\text{permutation of a set with } n \text{ elements}\}$$

$$SymmetricGroupOrder := o(S_n) = n!$$

$$SymmetricGroupAsDisjoinsCycles := \forall_{\sigma \in S_n} \exists_{\Sigma \subseteq S_n} \left( (DisjointCycles[\Sigma]) \wedge (\sigma = \prod(\sigma_i)) \right)$$

$$SymmetricGroupAsTranspositions := \forall_{\sigma \in S_n} \exists_{\Sigma \subseteq S_n} \left( (Transpositions[\Sigma]) \wedge (\sigma = \prod(\sigma_i)) \right)$$

$$vFunction[v(\sigma), \sigma, S_n] := v(\sigma) = n - |DisjointFullCycles[\Sigma]|$$

$$signFunction[sign(\sigma), \sigma, S_n] := sign(\sigma) = (-1)^{v(\sigma)}$$

$$EvenPermutation[\sigma, S_n] := sign(\sigma) = 1$$

$$OddPermutation[\sigma, S_n] := sign(\sigma) = -1$$

$$TranspositionSigns := sign(\tau\sigma) = -sign(\sigma)$$

$$TranspositionSignsCorollary := sign\left(\prod_{i=1}^r (\tau_i)\right) = (-1)^r$$

$$SignProp := sign(\sigma\pi) = sign(\sigma)sign(\pi)$$

$$AlternatingGroup[A_n, n] := A_n = \{\sigma \in S_n \mid EvenPermutation[\sigma, S_n]\}$$

$$AlternatingGroupOrder := o(A_n) = n!/2$$

## 2.5.3 Dihedral Group

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

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

## 2.6 Lagrange's Theorem

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

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

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

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

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

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

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

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

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

$$(2) \text{EqRel}[\sim, G]$$

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

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

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

$$\text{CosetSet}[G : H, H, G, *] := (\text{Subgroup}[H, G, *]) \wedge (G : H = \{gH \mid g \in G\})$$

$$\text{IndexSubgroup}[|G : H|, H, G, *] := (\text{CosetSet}[G : H, H, G, *]) \wedge (|G : H| = |G : H|) \wedge (|G| = (|H|)(|G : H|))$$

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

$$(1) (\text{CosetInduceEqRel}) \wedge (\text{EqRelInducesPartition}) \wedge (\text{CosetCardinality}) \blacksquare (o(G) = o(H)|G : H|) \wedge (\text{Divides}[o(H), o(G)])$$

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

$$(1) \text{CyclicSubgroup}[\langle g \rangle, g, G, *] \blacksquare \text{Order}[\langle g \rangle] = m$$

$$(2) (\text{LagrangeTheorem}) \wedge (\text{CyclicSubgroup}) \blacksquare \text{Divides}[\text{Order}[\langle g \rangle], \text{Order}[G]] \blacksquare \text{Divides}[m, n]$$

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

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

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

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

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

$$(1) (\text{LagrangeTheorem}) \wedge (\text{SubgroupIntersection}) \wedge (\text{RelPrime}(o(H), o(K))) \blacksquare H \cap K = \{e\}$$

## 2.7 Homomorphisms

$$\text{Homomorphism}[\phi, G, *, H, \diamond] := (\text{Function}[\phi, G, H]) \wedge \left( \forall_{a, b \in G} (\phi(a * b) = \phi(a) \diamond \phi(b)) \right)$$

$$\text{Monomorphism}[\phi, G, *, H, \diamond] := (\text{Homomorphism}[\phi, G, *, H, \diamond]) \wedge (\text{Inj}[\phi, G, H])$$

$$\text{Epimorphism}[\phi, G, *, H, \diamond] := (\text{Homomorphism}[\phi, G, *, H, \diamond]) \wedge (\text{Surj}[\phi, G, H])$$

$$\text{Isomorphism}[\phi, G, *, H, \diamond] := (\text{Homomorphism}[\phi, G, *, H, \diamond]) \wedge (\text{Bij}[\phi, G, H])$$

$$\text{Isomorphic}[G, *, H, \diamond] := \exists_{\phi} (\text{Isomorphism}[\phi, G, *, H, \diamond]) \text{ ** Notation: } G \cong H \text{ **}$$

$$\text{Automorphism}[\phi, G, *] := \text{Isomorphism}[\phi, G, *, G, *]$$

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

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

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

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

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

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

$$(1) \quad (n = 1) \implies \dots$$

$$(1.1) \quad \phi(g^n) = \phi(g) = \phi(g)^n \quad \blacksquare \quad \phi(g^n) = \phi(g)^n$$

$$(2) \quad (n = 1) \implies (\phi(g^n) = \phi(g)^n)$$

$$(3) \quad \left( \forall_{m \in \mathbb{N}^+} \left( (m \leq n) \implies (\phi(g^m) = \phi(g)^m) \right) \right) \implies \dots$$

$$(3.1) \quad \phi(g^{n+1}) = \phi(g^n * g) = \phi(g)^n \diamond \phi(g) = \phi(g)^{n+1} \quad \blacksquare \quad \phi(g^{n+1}) = \phi(g)^{n+1}$$

$$(4) \quad \left( \forall_{m \in \mathbb{N}^+} \left( (m \leq n) \implies (\phi(g^m) = \phi(g)^m) \right) \right) \implies (\phi(g^{n+1}) = \phi(g)^{n+1})$$

$$(5) \quad \left( (n = 1) \implies (\phi(g^n) = \phi(g)^n) \right) \wedge \left( \left( \forall_{m \in \mathbb{N}^+} \left( (m \leq n) \implies (\phi(g^m) = \phi(g)^m) \right) \right) \implies (\phi(g^{n+1}) = \phi(g)^{n+1}) \right) \dots$$

$$(6) \quad \dots \forall_{n \in \mathbb{N}^+} (\phi(g^n) = \phi(g)^n)$$

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

$$(1) \quad OrderElDivOrder \quad \blacksquare \quad g^n = e_G$$

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

$$(3) \quad (ExpModOrderCorollary) \wedge (OrderEl[m, \phi(g), H, \diamond]) \wedge (\phi(g)^n = e_H) \quad \blacksquare \quad Divides[m, n]$$

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

$$(1) \quad Inj[\phi, G, H] \quad \blacksquare \quad \forall_{g_1, g_2 \in G} \left( (\phi(g_1) = \phi(g_2)) \implies (g_1 = g_2) \right)$$

$$(2) \quad e_H = \phi(g)^m = \phi(g^m) \quad \blacksquare \quad e_H = \phi(g^m)$$

$$(3) \quad e_H = \phi(e_G) = \phi(g^n) \quad \blacksquare \quad e_H = \phi(g^n)$$

$$(4) \quad \left( \forall_{g_1, g_2 \in G} \left( (\phi(g_1) = \phi(g_2)) \implies (g_1 = g_2) \right) \right) \wedge (e_H = \phi(g^m)) \wedge (e_H = \phi(g^n)) \quad \blacksquare \quad g^m = g^n$$

$$(5) \quad (OrderEl[m, \phi(g), H, \diamond]) \wedge (Order[n, G, *]) \wedge (g^m = g^n) \quad \blacksquare \quad m = n$$

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

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

$$(2) \quad (g_1, g_2 \in G) \implies \dots$$

$$(2.1) \quad (Homomorphism[\phi, G, *, H, \diamond]) \wedge (Homomorphism[\theta, H, \diamond, K, \square]) \quad \blacksquare \quad \theta \circ \phi(g_1 * g_2) = \theta(\phi(g_1 * g_2)) = \dots$$

$$(2.2) \quad \dots \theta(\phi(g_1) \diamond \phi(g_2)) = \theta(\phi(g_1)) \square \theta(\phi(g_2)) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2) \quad \blacksquare \quad \theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2)$$

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

$$(4) \quad (Func[\theta \circ \phi, G, K]) \wedge \left( \forall_{g_1, g_2 \in G} (\theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2)) \right) \quad \blacksquare \quad Homomorphism[\theta \circ \phi, G, *, K, \square]$$

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

$$(1) \quad Isomorphism[\phi, G, *, H, \diamond] \quad \blacksquare \quad (Homomorphism[\phi, G, *, H, \diamond]) \wedge (Bij[\phi, G, H])$$

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

$$(3) \quad (x, y \in H) \implies \dots$$

$$(3.1) \quad Homomorphism[\phi, G, *, H, \diamond] \quad \blacksquare \quad \phi(\phi^{-1}(x) * \phi^{-1}(y)) = \phi(\phi^{-1}(x)) \diamond \phi(\phi^{-1}(y)) = x \diamond y$$

$$(3.2) \quad \phi^{-1}(x \diamond y) = \phi^{-1}\left(\phi\left(\phi^{-1}(x) * \phi^{-1}(y)\right)\right) = (\phi^{-1} \circ \phi)\left(\phi^{-1}(x) * \phi^{-1}(y)\right) = \phi^{-1}(x) * \phi^{-1}(y) \quad \blacksquare \quad \phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y)$$

$$(4) \quad (x, y \in H) \implies \left(\phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y)\right) \quad \blacksquare \quad \forall_{x, y \in H} \left(\phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y)\right)$$

$$(5) \quad (Bij[\phi^{-1}, H, G]) \wedge \left(\forall_{x, y \in H} \left(\phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y)\right)\right) \quad \blacksquare \quad Isomorphism[\phi^{-1}, H, \diamond, G, *]$$

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

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

$$(2) \quad \phi := \{\langle g^n, h^n \rangle \in (G \times H) \mid n \in \mathbb{Z}\}$$

$$(3) \quad (n_1, n_2 \in \mathbb{Z}) \implies \dots$$

$$(3.1) \quad (ExpModOrder) \wedge (Order[n, G, *]) \wedge (Order[n, H, \diamond]) \quad \blacksquare \quad (g^{n_1} = g^{n_2}) \iff (n_1 \equiv n_2 \pmod{n}) \iff (h^{n_1} = h^{n_2}) \iff \dots$$

$$(3.2) \quad \dots (\phi(g^{n_1}) = \phi(g^{n_2})) \quad \blacksquare \quad (g^{n_1} = g^{n_2}) \iff (\phi(g^{n_1}) = \phi(g^{n_2}))$$

$$(4) \quad (n_1, n_2 \in \mathbb{Z}) \implies \left((g^{n_1} = g^{n_2}) \iff (\phi(g^{n_1}) = \phi(g^{n_2}))\right) \dots$$

$$(5) \quad \dots (Func[\phi, G, H]) \wedge (Inj[\phi, G, H]) \wedge (Surj[\phi, G, H]) \quad \blacksquare \quad Bij[\phi, G, H]$$

$$(6) \quad (g^n, g^m \in G) \implies \dots$$

$$(6.1) \quad \phi(g^n * g^m) = \phi(g^{n+m}) = h^{n+m} = h^n \diamond h^m = \phi(g^n) \diamond \phi(g^m) \quad \blacksquare \quad \phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m)$$

$$(7) \quad (g^n, g^m \in G) \implies (\phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m)) \quad \blacksquare \quad \forall_{g^n, g^m \in G} (\phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m))$$

$$(8) \quad (Bij[\phi, G, H]) \wedge \left(\forall_{g^n, g^m \in G} (\phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m))\right) \quad \blacksquare \quad Isomorphism[\phi, G, *, H, \diamond]$$

$$(9) \quad \exists_{\phi} (Isomorphism[\phi, G, *, H, \diamond]) \quad \blacksquare \quad Isomorphic[G, *, H, \diamond]$$

## 2.8 Kernel and Image Homomorphisms

$$Kernel[ker_{\phi}, \phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \wedge \left(ker_{\phi} = \{g \in G \mid \phi(g) = e_H\}\right)$$

$$Image[im_{\phi}, \phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \wedge \left(im_{\phi} = \{\phi(g) \in H \mid g \in G\}\right)$$

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

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

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

$$(3) \quad (a, b \in ker_{\phi}) \implies \dots$$

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

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

$$(5) \quad (a \in ker_{\phi}) \implies \dots$$

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

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

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

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

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

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

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

$$(3) \quad (a, b \in im_{\phi}) \implies \dots$$

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

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

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

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

- 
- (1)  $CyclicGroup[G, *] \blacksquare \exists_{r \in G} (Generator[r, G, *]) \blacksquare G = \langle r \rangle = \{r^n \mid n \in \mathbb{Z}\}$
- 
- (2)  $ExpMapsExp \blacksquare im_\phi = \{\phi(g) \mid g \in G\} = \{\phi(r^n) \mid n \in \mathbb{Z}\} = \{\phi(r)^n \mid n \in \mathbb{Z}\} = \langle \phi(r) \rangle$
- 
- (3)  $Generator[\phi(r), im_\phi, \diamond] \blacksquare \exists_{s \in im_\phi} (Generator[s, im_\phi, \diamond]) \blacksquare CyclicGroup[im_\phi, \diamond]$
- 

$$HomoInjEquiv := (Homomorphism[\phi, G, *, H, \diamond]) \implies ((Inj[\phi, G, H]) \iff (ker_\phi = \{e_G\}))$$

- 
- (1)  $(Inj[\phi, G, H]) \implies \dots$
- 
- (1.1)  $IdMapsId \blacksquare \phi(e_G) = e_H \blacksquare e_G \in ker_\phi \blacksquare \{e_G\} \subseteq ker_\phi$
- 
- (1.2)  $(g \in ker_\phi) \implies \dots$
- 
- (1.2.1)  $(g \in ker_\phi) \wedge (IdMapsId) \blacksquare \phi(g) = e_H = \phi(e_G)$
- 
- (1.2.2)  $(Inj[\phi, G, H]) \wedge (\phi(g) = \phi(e_G)) \blacksquare g = e_G \blacksquare g \in \{e_G\}$
- 
- (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)  $(Inj[\phi, G, H]) \implies (ker_\phi = \{e_G\})$
- 
- (3)  $(ker_\phi = \{e_G\}) \implies \dots$
- 
- (3.1)  $((g_1, g_2 \in G) \wedge (\phi(g_1) = \phi(g_2))) \implies \dots$
- 
- (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)  $(ker_\phi = \{e_G\}) \wedge (g_1 * g_2^{-1} \in ker_\phi) \blacksquare g_1 * g_2^{-1} = e_G \blacksquare g_1 = g_2$
- 
- (3.2)  $((g_1, g_2 \in G) \wedge (\phi(g_1) = \phi(g_2))) \implies (g_1 = g_2) \blacksquare \forall_{g_1, g_2 \in G} ((\phi(g_1) = \phi(g_2)) \implies (g_1 = g_2)) \blacksquare Inj[\phi, G, H]$
- 
- (4)  $(ker_\phi = \{e_G\}) \implies (Inj[\phi, G, H])$
- 
- (5)  $((Inj[\phi, G, H]) \implies (ker_\phi = \{e_G\})) \wedge ((ker_\phi = \{e_G\}) \implies (Inj[\phi, G, H]))$
- 
- (6)  $(Inj[\phi, G, H]) \iff (ker_\phi = \{e_G\})$
- 

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

- 
- (1)  $(x \in (ker_\phi)g) \implies \dots$
- 
- (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)  $(x \in (ker_\phi)g) \implies (\phi(x) = \phi(g)) \blacksquare (ker_\phi)g \subseteq \{x \in G \mid \phi(x) = \phi(g)\}$
- 
- (3)  $((x \in G) \wedge (\phi(x) = \phi(g))) \implies \dots$
- 
- (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)  $((x \in G) \wedge (\phi(x) = \phi(g))) \implies (x \in (ker_\phi)g) \blacksquare \{x \in G \mid \phi(x) = \phi(g)\} \subseteq (ker_\phi)g$
- 
- (5)  $((ker_\phi)g \subseteq \{x \in G \mid \phi(x) = \phi(g)\}) \wedge (\{x \in G \mid \phi(x) = \phi(g)\} \subseteq (ker_\phi)g) \blacksquare (ker_\phi)g = \{x \in G \mid \phi(x) = \phi(g)\}$
-

$$\text{KerImPartitions}G := (\text{Homomorphism}[\phi, G, *, H, \diamond]) \implies (|G| = |\ker_\phi| |\text{im}_\phi|)$$

$$(1) \quad \forall_{g \in G} ([g] = \{x \in G \mid \phi(x) = \phi(g)\})$$

$$(2) \quad \mathcal{G} = \{[g] \mid g \in G\} \quad \blacksquare \quad (\text{Partition}[\mathcal{G}, G]) \wedge (|\mathcal{G}| = |\text{im}_\phi|)$$

$$(3) \quad \text{KerMultiplicityMap} \quad \blacksquare \quad \forall_{g \in G} (|[g]| = |\ker_\phi|)$$

$$(4) \quad \text{Partition}[\mathcal{G}, G] \quad \blacksquare \quad |G| = |\mathcal{G}| |\ker_\phi| = |\text{im}_\phi| |\ker_\phi|$$

$$\text{ImDivDomCod} := (\text{Homomorphism}[\phi, G, *, H, \diamond]) \implies \left( (\text{Divides}[|\text{im}_\phi|, |G|]) \wedge (\text{Divides}[|\text{im}_\phi|, |H|]) \right)$$

$$(1) \quad \text{KerImPartitions}G \quad \blacksquare \quad |G| = |\ker_\phi| |\text{im}_\phi| \quad \blacksquare \quad \text{Divides}[|\text{im}_\phi|, |G|]$$

$$(2) \quad (\text{LagrangeTheorem}) \wedge (\text{ImageSubgroupCodomain}) \quad \blacksquare \quad |H| = |\text{im}_\phi| |H : \text{im}_\phi| \quad \text{Divides}[|\text{im}_\phi|, |H|]$$

## 2.9 Conjugacy

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

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

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

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

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

$$(1.3) \quad ((a \sim^* b) \wedge (b \sim^* c)) \implies \left( (b = x_b^{-1} * a * x_b) \wedge (c = x_c^{-1} * b * x_c) \right) \implies \dots$$

$$(1.4) \quad \dots \left( c = x_c^{-1} * x_b^{-1} * a * x_b * x_c = (x_b * x_c)^{-1} * a * (x_b * x_c) \right) \quad \blacksquare \quad a \sim^* c$$

$$(2) \quad \text{EqRel}[\sim^*, G]$$

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

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

$$(1) \quad \text{By } \text{ConjugateEqRel} \text{ and the definitions of } \text{ConjugacyClass}, \text{Conjugate}$$

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

$$(1) \quad (C_g = \{g\}) \implies \dots$$

$$(1.1) \quad (x \in G) \implies \dots$$

$$(1.1.1) \quad (\text{ConjugacyClass}[C_g, g, G, *]) \wedge (\text{ConjugacyClassEquiv}) \wedge (x \in G) \quad \blacksquare \quad x^{-1} g x \in C_g$$

$$(1.1.2) \quad (C_g = \{g\}) \wedge (x^{-1} g x \in C_g) \quad \blacksquare \quad x^{-1} g x = g \quad \blacksquare \quad g x = x g$$

$$(1.2) \quad (x \in G) \implies (g x = x g) \quad \blacksquare \quad \forall_{x \in G} (g x = x g) \quad \blacksquare \quad g \in Z(G)$$

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

$$(3) \quad (g \in Z(G)) \implies \dots$$

$$(3.1) \quad (g \in Z(G)) \wedge (\text{Group}[G, *]) \quad \blacksquare \quad (\forall_{c \in G} (g c = c g)) \wedge (\exists_e (e \in G))$$

$$(3.2) \quad (x \in G) \implies \dots$$

$$(3.2.1) \quad (\forall_{c \in G} (g c = c g)) \wedge (\exists_e (e \in G)) \quad \blacksquare \quad \left( \exists_{c \in G} (x = c^{-1} g c) \right) \iff \left( \exists_{c \in G} (x = c^{-1} g c = c^{-1} c g = g) \right) \iff (x = g) \iff (x \in \{g\})$$

$$(3.3) \quad (x \in G) \implies \left( \left( \exists_{c \in G} (x = c^{-1} g c) \right) \iff (x \in \{g\}) \right) \quad \blacksquare \quad \forall_{x \in G} \left( (x \in \{g\}) \iff \left( \exists_{c \in G} (x = c^{-1} g c) \right) \right)$$

$$(3.4) \quad (\text{ConjugacyClassEquiv}) \wedge \left( \forall_{x \in G} \left( (x \in \{g\}) \iff \left( \exists_{c \in G} (x = c^{-1} g c) \right) \right) \right) \quad \blacksquare \quad C_g = \{g\}$$

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

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



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

$$(1) \quad \text{ConjugacyCenter} \quad \blacksquare \left( \forall_{g \in G} (C_g = \{g\}) \right) \iff \left( \forall_{g \in G} (g \in Z(G)) \right) \iff (\text{AbelianGroup}[G, *])$$

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

$$(1) \quad (n = 1) \implies \dots$$

$$(1.1) \quad (x^{-1}gx)^n = (x^{-1}gx)^1 = x^{-1}g^1x = x^{-1}g^nx \quad \blacksquare \quad (x^{-1}gx)^n = x^{-1}g^nx$$

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

$$(3) \quad \left( (n > 1) \wedge \left( \forall_{m \in \mathbb{N}^+} \left( (m \leq n) \implies \left( (x^{-1}gx)^m = x^{-1}g^mx \right) \right) \right) \right) \implies \dots$$

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

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

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

$$\text{ConjugateOrder} := ((g_1, g_2 \in G) \wedge (g_1 \sim^* g_2)) \implies (o(g_1) = o(g_2))$$

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

$$(2) \quad \text{ConjugateExp} \quad \blacksquare \quad e = g_2^{o(g_2)} = (c^{-1}g_1c)^{o(g_2)} = c^{-1}g_1^{o(g_2)}c \quad \blacksquare \quad e = c^{-1}g_1^{o(g_2)}c \quad \blacksquare \quad g_1^{o(g_2)} = e$$

$$(3) \quad \text{ExpModOrderCorollary} \quad \blacksquare \quad \text{Divides}[o(g_2), o(g_1)]$$

$$(4) \quad \text{ConjugateExp} \quad \blacksquare \quad e = g_1^{o(g_1)} = (cg_2c^{-1})^{o(g_1)} = cg_2^{o(g_1)}c^{-1} \quad \blacksquare \quad e = cg_2^{o(g_1)}c^{-1} \quad \blacksquare \quad g_2^{o(g_1)} = e$$

$$(5) \quad \text{ExpModOrderCorollary} \quad \blacksquare \quad \text{Divides}[o(g_1), o(g_2)]$$

$$(6) \quad (\text{Divides}[o(g_2), o(g_1)]) \wedge (\text{Divides}[o(g_1), o(g_2)]) \wedge (g_1, g_2 \in \mathbb{N}^+) \quad \blacksquare \quad o(g_1) = o(g_2)$$

$$(7) \quad \text{=====}$$

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

$$(9) \quad (m \in \mathbb{Z}^+) \wedge (m < o(g_2)) \implies \dots$$

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

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

$$(11) \quad (g_1^{o(g_2)} = e) \wedge \left( \forall_{m \in \mathbb{Z}^+} \left( (m < o(g_2)) \implies (g_1^m \neq e) \right) \right) \quad \blacksquare \quad o(g_1) = o(g_2)$$

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

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

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

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

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

$$(3) \quad (a \in C(h)) \implies \dots$$

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

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

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

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

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

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

$$(2) \quad (x, y \in G) \implies \dots$$

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

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

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

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

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

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

## 2.10 Normal Subgroups

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

$$\text{CenterNormalSubgroup} := \text{NormalSubgroup}[Z(G), G, *]$$

$$(1) \quad \text{SubgroupCenter} \blacksquare \text{Subgroup}[Z(G), G, *]$$

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

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

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

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

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

$$(1) \quad (\text{NormalSubgroup}[H, G, *]) \implies \dots$$

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

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

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

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

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

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

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

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

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

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

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

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

$$(1) \quad CosetCardinality \blacksquare \forall_{g \in G} (|Hg| = |gH|) \blacksquare \left( \forall_{g \in G} ((Hg \subseteq gH) \iff (Hg = gH)) \right)$$

$$(2) \quad \left( \forall_{g \in G} ((Hg \subseteq gH) \iff (Hg = gH)) \right) \blacksquare (NormalSubgroup[H, G, *]) \iff \left( \forall_{h \in H} \forall_{g \in G} (g^{-1}hg \in H) \right) \iff \dots$$

$$(3) \quad \dots \left( \forall_{h \in H} \forall_{g \in G} (hg \in gH) \right) \iff \left( \forall_{g \in G} (Hg \subseteq gH) \right) \iff \left( \forall_{g \in G} (Hg = gH) \right)$$

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

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

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

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

$$(2) \quad \left( (h \in ker_\phi) \wedge (g \in G) \right) \implies \dots$$

$$(2.1) \quad h \in ker_\phi \blacksquare \phi(h) = e_H$$

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

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

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

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

## 2.11 Quotient Groups

$$QuotientSet[G/H, H, G, *] := (Subgroup[H, G, *]) \wedge (G/H = \{Hg \mid g \in G\})$$

$$CosetMul[\bar{*}, H, G, *] := (Subgroup[H, G, *]) \wedge \left( \forall_{Hx, Hy \in G/H} (Hx \bar{*} Hy = \{h_1 x h_2 y \mid h_1, h_2 \in H\}) \right)$$

$$SubsetMul[\bar{\times}, G, *] := (Group[G, *]) \wedge \left( \forall_{A, B \subseteq G} (A \bar{\times} B = \{a * b \mid (a \in A) \wedge (b \in B)\}) \right)$$

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

$$(1) \quad \left( \exists_{h_1, h_2 \in H} (z = h_1 x h_2 y) \right) \implies \dots$$

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

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

$$(1.3) \quad (Group[H, *]) \wedge (h_1, x h_2 x^{-1} \in H) \blacksquare h_1 x h_2 x^{-1} \in H$$

$$(1.4) \quad (h_1 x h_2 x^{-1})(xy) = h_1 x h_2 y = z \blacksquare (h_1 x h_2 x^{-1})(xy) = z$$

$$(1.5) \quad (h_1 x h_2 x^{-1} \in H) \wedge \left( (h_1 x h_2 x^{-1})(xy) = z \right) \blacksquare \exists_{h_3 \in H} (z = h_3 xy)$$

$$(2) \quad \left( \exists_{h_1, h_2 \in H} (z = h_1 x h_2 y) \right) \implies \left( \exists_{h_3 \in H} (z = h_3 xy) \right)$$

$$(3) \quad \left( \exists_{h_3 \in H} (z = h_3 xy) \right) \implies \dots$$

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

$$(3.2) \quad Group[H, *] \blacksquare e \in H$$

$$(3.3) \quad (e)x(x^{-1} h_3 x)y = h_3 xy = z \blacksquare (e)x(x^{-1} h_3 x)y = z$$

$$(3.4) \quad (x^{-1} h_3 x, e \in H) \wedge \left( (e)x(x^{-1} h_3 x)y = h_3 xy = z \right) \blacksquare \exists_{h_1, h_2 \in H} (z = h_1 x h_2 y)$$

$$(4) \quad \left( \exists_{h_3 \in H} (z = h_3 xy) \right) \implies \left( \exists_{h_1, h_2 \in H} (z = h_1 x h_2 y) \right)$$

$$(5) \quad \left( \left( \exists_{h_1, h_2 \in H} (z = h_1 x h_2 y) \right) \implies \left( \exists_{h_3 \in H} (z = h_3 x y) \right) \right) \wedge \left( \left( \exists_{h_3 \in H} (z = h_3 x y) \right) \implies \left( \exists_{h_1, h_2 \in H} (z = h_1 x h_2 y) \right) \right)$$

$$(6) \quad \left( \exists_{h_1, h_2 \in H} (z = h_1 x h_2 y) \right) \iff \left( \exists_{h_3 \in H} (z = h_3 x y) \right)$$

$$\text{QuotientGroupThm} := \left( \left( \text{NormalSubgroup}[H, G, *] \wedge \left( \text{QuotientSet}[G/H, H, G, *] \wedge \left( \text{CosetMul}[\bar{*}, x, y, H, G, *] \right) \implies \right) \right) \right)$$

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

$$(1.1) \quad (\text{NormalSubgroup}[H, G, *] \wedge (\text{QuotientGroupLemma}) \blacksquare \forall_{x, y, z \in G} \left( \left( \exists_{h_1, h_2 \in H} (z = h_1 x h_2 y) \right) \iff \left( \exists_{h_3 \in H} (z = h_3 x y) \right) \right))$$

$$(1.2) \quad (z \in Hx \bar{*} Hy) \iff \left( \exists_{h_1, h_2 \in H} (z = h_1 x h_2 y) \right) \iff \left( \exists_{h_3 \in H} (z = h_3 x y) \right) \iff (z \in Hxy) \blacksquare Hx \bar{*} Hy = Hxy$$

$$(1.3) \quad (\text{Group}[G, *]) \wedge (x, y \in G) \blacksquare xy \in G \blacksquare Hxy \in G/H$$

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

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

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

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

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

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

$$(6) \quad (Hx \in G/H) \implies \dots$$

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

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

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

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

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

$$(9) \quad \dots \left( \forall_{a \in G/H} \exists_{a^{-1} \in G/H} (a \bar{*} a^{-1} = e = a^{-1} \bar{*} a) \right) \blacksquare \text{Group}[G/H, \bar{*}]$$

$$\text{NaturalMap}[\bar{\phi}, H, G, *] := (\bar{\phi} = \{\langle g, Hg \rangle \in (G, G/H) \mid g \in G\}) \wedge (\text{NormalSubgroup}[H, G, *])$$

$$\text{NaturalMapHomo} := (\text{NaturalMap}[\bar{\phi}, H, G, *]) \implies (\text{Homomorphism}[\bar{\phi}, G, *, G/H, \bar{*}])$$

$$(1) \quad \text{NaturalMap}[\bar{\phi}, H, G, *] \blacksquare \text{Func}[\bar{\phi}, G, *, G/H, \bar{*}]$$

$$(2) \quad (x, y \in G) \implies \dots$$

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

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

$$(4) \quad (\text{Func}[\bar{\phi}, G, *, G/H, \bar{*}]) \wedge \left( \forall_{x, y \in G} (\bar{\phi}(x) \bar{*} \bar{\phi}(y)) \right) \blacksquare \text{Homomorphism}[\bar{\phi}, G, *, G/H, \bar{*}]$$

$$\text{NaturalMapKerH} := (\text{NaturalMap}[\bar{\phi}, H, G, *]) \implies (\ker_{\bar{\phi}} = H)$$

$$(1) \quad \text{Group}[H, *] \blacksquare \ker_{\bar{\phi}} = \{x \in G \mid \bar{\phi}(x) = He\} = \{x \in G \mid Hx = H\} = H$$

$$\text{FirstMap}[\psi, \phi, G, *, H, \diamond] := \left( \psi = \{\langle \ker_{\phi} g, \phi(g) \rangle \in (G/\ker_{\phi} \times \text{im}_{\phi}) \mid g \in G\} \right) \wedge (\text{Homomorphism}[\phi, G, *, H, \diamond])$$

$$\text{FirstIsoThm} := (\text{Homomorphism}[\phi, G, *, H, \diamond]) \implies (\text{Isomorphic}[G/\ker_{\phi}, \bar{*}, \text{im}_{\phi}, \diamond])$$

$$(1) \quad (\text{KerInduceNormalSubgroup}) \wedge (\text{Homomorphism}[\phi, G, *, H, \diamond]) \blacksquare \text{NormalSubgroup}[\ker_{\phi}, G, *]$$

$$(2) \quad (\text{QuotientGroupThm}) \wedge (\text{NormalSubgroup}[\ker_{\phi}, G, *]) \blacksquare \text{Group}[G/\ker_{\phi}, \bar{*}]$$

$$(3) \quad (\text{ImageSubgroupCodomain}) \wedge (\text{Homomorphism}[\phi, G, *, H, \diamond]) \blacksquare \text{Group}[\text{im}_{\phi}, \diamond]$$

$$(4) \quad \text{FirstMap}[\psi, \phi, G, *, H, \diamond] \blacksquare \psi = \{\langle \ker_{\phi} g, \phi(g) \rangle \in (G/\ker_{\phi} \times \text{im}_{\phi}) \mid g \in G\}$$

$$(5) \quad (g, h \in G) \implies \dots$$

$$(5.1) \quad (\ker_{\phi} g = \ker_{\phi} h) \iff (\ker_{\phi} gh^{-1} = \ker_{\phi}) \iff (gh^{-1} \in \ker_{\phi}) \iff (\phi(gh^{-1}) = e_H) \iff \dots$$

$$(5.2) \quad \dots \left( e_H = \phi(g) \diamond \phi(h^{-1}) = \phi(g) \diamond \phi(h)^{-1} \right) \iff (\phi(g) = \phi(h)) \quad \blacksquare \quad (\ker_{\phi} g = \ker_{\phi} h) \iff (\phi(g) = \phi(h))$$

$$(6) \quad (g, h \in G) \implies \left( (\ker_{\phi} g = \ker_{\phi} h) \iff (\phi(g) = \phi(h)) \right) \dots$$

$$(7) \quad \dots (\text{Func}[\psi, G/\ker_{\phi}, \text{im}_{\phi}] \wedge (\text{Inj}[\psi, G/\ker_{\phi}, \text{im}_{\phi}] \wedge (\text{Surj}[\psi, G/\ker_{\phi}, \text{im}_{\phi}] \quad \blacksquare \quad \text{Bij}[\psi, G/\ker_{\phi}, \text{im}_{\phi}]))$$

$$(8) \quad (\ker_{\phi} g, \ker_{\phi} h \in G/\ker_{\phi}) \implies \dots$$

$$(8.1) \quad \psi(\ker_{\phi} g \bar{*} \ker_{\phi} h) = \psi(\ker_{\phi} gh) = \phi(g * h) = \phi(g) \diamond \phi(h) = \psi(\ker_{\phi} g) \diamond \psi(\ker_{\phi} h) \quad \blacksquare \quad \psi(\ker_{\phi} g \bar{*} \ker_{\phi} h) = \psi(\ker_{\phi} g) \diamond \psi(\ker_{\phi} h)$$

$$(9) \quad (\ker_{\phi} g, \ker_{\phi} h \in G/\ker_{\phi}) \implies \left( \psi(\ker_{\phi} g \bar{*} \ker_{\phi} h) = \psi(\ker_{\phi} g) \diamond \psi(\ker_{\phi} h) \right) \quad \blacksquare \quad \forall_{a,b \in G/\ker_{\phi}} (\psi(a \bar{*} b) = \psi(a) \diamond \psi(b))$$

$$(10) \quad (\text{Group}[G/\ker_{\phi}, \bar{*}]) \wedge (\text{Group}[\text{im}_{\phi}, \diamond]) \wedge (\text{Bij}[\psi, G/\ker_{\phi}, \text{im}_{\phi}]) \wedge \left( \forall_{a,b \in G/\ker_{\phi}} (\psi(a \bar{*} b) = \psi(a) \diamond \psi(b)) \right)$$

$$(11) \quad \text{Isomorphism}[\psi, G/\ker_{\phi}, \bar{*}, \text{im}_{\phi}, \diamond] \quad \blacksquare \quad \exists_{\psi} (\text{Isomorphism}[\psi, G/\ker_{\phi}, \bar{*}, \text{im}_{\phi}, \diamond]) \quad \blacksquare \quad \text{Isomorphic}[G/\ker_{\phi}, \bar{*}, \text{im}_{\phi}, \diamond]$$

$$\text{Second Iso Lemma} := ((\text{Subgroup}[H, G, *]) \wedge (\text{NormalSubgroup}[N, G, *])) \implies \left( (\text{Group}[(HN)/N, \bar{*}]) \wedge (\text{Group}[H/(H \cap N), \bar{*}]) \right)$$

$$(1) \quad (\text{Group}[H, *]) \wedge (\text{Group}[N, *]) \quad \blacksquare \quad (e \in H) \wedge (e \in N)$$

$$(2) \quad e = e * e \in HN \quad \blacksquare \quad \emptyset \neq HN \subseteq G$$

$$(3) \quad (h_1 n_1, h_2 n_2 \in HN) \implies \dots$$

$$(3.1) \quad h_2 \in G \quad \blacksquare \quad (h_2)^{-1} n_1 h_2 \in N$$

$$(3.2) \quad (h_1 n_1)(h_2 n_2) = h_1 \left( h_2 (h_2)^{-1} \right) n_1 h_2 n_2 = (h_1 h_2) \left( (h_2)^{-1} n_1 h_2 n_2 \right) \quad \blacksquare \quad (h_1 n_1)(h_2 n_2) = (h_1 h_2) \left( (h_2)^{-1} n_1 h_2 n_2 \right)$$

$$(3.3) \quad (\text{Group}[H, *]) \wedge (\text{Group}[N, *]) \quad \blacksquare \quad (h_1 h_2 \in H) \wedge \left( (h_2)^{-1} n_1 h_2 n_2 \in N \right)$$

$$(3.4) \quad (h_1 n_1)(h_2 n_2) = (h_1 h_2) \left( (h_2)^{-1} n_1 h_2 n_2 \in N \quad \blacksquare \quad (h_1 n_1)(h_2 n_2) \in N \right)$$

$$(4) \quad (h_1 n_1, h_2 n_2 \in HN) \implies \left( (h_1 n_1)(h_2 n_2) \in N \right) \quad \blacksquare \quad \forall_{h_1 n_1, h_2 n_2 \in HN} \left( (h_1 n_1)(h_2 n_2) \in N \right)$$

$$(5) \quad (hn \in HN) \implies \dots$$

$$(5.1) \quad (\text{Subgroup}[H, G, *]) \wedge (\text{Group}[N, *]) \quad \blacksquare \quad (h^{-1} \in G) \wedge (n^{-1} \in N)$$

$$(5.2) \quad (\text{NormalSubgroup}[N, G, *]) \wedge (h^{-1} \in G) \wedge (n^{-1} \in N) \quad \blacksquare \quad hn^{-1}h^{-1} \in N$$

$$(5.3) \quad (hn)^{-1} = n^{-1}h^{-1} = (h^{-1}h)n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}) \in HN \quad \blacksquare \quad (hn)^{-1} \in HN$$

$$(6) \quad (hn \in HN) \implies \left( (hn)^{-1} \in HN \right) \quad \blacksquare \quad \forall_{hn \in HN} \left( (hn)^{-1} \in HN \right)$$

$$(7) \quad (\emptyset \neq HN \subseteq G) \wedge \left( \forall_{h_1 n_1, h_2 n_2 \in HN} \left( (h_1 n_1)(h_2 n_2) \in N \right) \right) \wedge \left( \forall_{hn \in HN} \left( (hn)^{-1} \in HN \right) \right) \quad \blacksquare \quad \text{Subgroup}[HN, G, *] \quad \blacksquare \quad \text{Group}[HN, *]$$

$$(8) \quad (N \subseteq HN) \wedge (\text{Group}[N, *]) \quad \blacksquare \quad \text{Subgroup}[N, HN, *]$$

$$(9) \quad ((n \in N) \wedge (h_1 n_1 \in HN)) \implies \dots$$

$$(9.1) \quad (\text{NormalSubgroup}[N, G, *]) \wedge (h_1 n_1 \in G) \quad \blacksquare \quad (h_1 n_1)^{-1} n (h_1 n_1) \in N$$

$$(10) \quad ((n \in N) \wedge (h_1 n_1 \in HN)) \implies \left( (h_1 n_1)^{-1} n (h_1 n_1) \in N \right) \quad \blacksquare \quad \forall_{n \in N} \forall_{h_1 n_1 \in HN} \left( (h_1 n_1)^{-1} n (h_1 n_1) \in N \right)$$

$$(11) \quad (\text{Subgroup}[N, HN, *]) \wedge \left( \forall_{n \in N} \forall_{h_1 n_1 \in HN} \left( (h_1 n_1)^{-1} n (h_1 n_1) \in N \right) \right) \quad \blacksquare \quad \text{NormalSubgroup}[N, HN, *]$$

$$(12) \quad (\text{SubgroupIntersection}) \wedge (\text{Subgroup}[H, G, *]) \wedge (\text{Subgroup}[N, G, *]) \quad \blacksquare \quad \text{Subgroup}[H \cap N, G, *] \quad \blacksquare \quad \text{Group}[H \cap N, *]$$

$$(13) \quad (H \cap N \subseteq H) \wedge (\text{Group}[H \cap N, *]) \quad \blacksquare \quad \text{Subgroup}[H \cap N, H, *]$$

$$(14) \quad ((x \in H \cap N) \wedge (h \in H)) \implies \dots$$

$$(14.1) \quad x \in H \cap N \quad \blacksquare \quad (x \in H) \wedge (x \in N)$$

$$(14.2) \quad (\text{Group}[H, *]) \wedge (h \in H) \quad \blacksquare \quad h^{-1} \in H$$

$$(14.3) \quad (\text{Group}[H, *]) \wedge (x, h, h^{-1} \in H) \quad \blacksquare \quad h^{-1} x h \in H$$

$$(14.4) \quad (\text{NormalSubgroup}[N, G, *]) \wedge (h \in G) \wedge (x \in N) \quad \blacksquare \quad h^{-1} x h \in N$$

$$(14.5) \quad (h^{-1} x h \in H) \wedge (h^{-1} x h \in N) \quad \blacksquare \quad h^{-1} x h \in H \cap N$$

$$(15) \quad ((x \in H \cap N) \wedge (h \in H)) \implies (h^{-1} x h \in H \cap N) \quad \blacksquare \quad \forall_{x \in H \cap N} \forall_{h \in H} (h^{-1} x h \in H \cap N)$$

$$(16) \quad (\text{Subgroup}[H \cap N, H, *]) \wedge \left( \forall_{x \in H \cap N} \forall_{h \in H} (h^{-1} x h \in H \cap N) \right) \quad \blacksquare \quad \text{NormalSubgroup}[H \cap N, H, *]$$

$$(17) \quad (\text{Group}[HN, *]) \wedge (\text{NormalSubgroup}[N, HN, *]) \wedge (\text{Group}[H, *]) \wedge (\text{NormalSubgroup}[H \cap N, H, *])$$

$$(18) \text{ QuotientGroupThm } \blacksquare \left( \text{Group}[(HN)/N, \bar{*}] \right) \wedge \left( \text{Group}[H/(H \cap N), \bar{*}] \right)$$

$$\text{SecondMap}[\phi, H, N, G, *] := \left( \phi = \{ \langle h, hN \rangle \in (H \times (HN)/N) \mid h \in H \} \right) \wedge (\text{Subgroup}[H, G, *]) \wedge (\text{NormalSubgroup}[N, G, *])$$

$$\text{SecondIsoThm} := ((\text{Subgroup}[H, G, *]) \wedge (\text{NormalSubgroup}[N, G, *])) \implies (\text{Isomorphic}[H/(H \cap N), \bar{*}, (HN)/N, \bar{*}])$$

$$(1) \text{ SecondIsoLemma } \blacksquare \left( \text{Group}[(HN)/N, \bar{*}] \right) \wedge \left( \text{Group}[H/(H \cap N), \bar{*}] \right)$$

$$(2) \text{ SecondMap}[\phi, H, N, G, *] \blacksquare \phi = \{ \langle h, hN \rangle \in (H \times (HN)/N) \mid h \in H \}$$

$$(3) ((h_1, h_2 \in H) \wedge (h_1 = h_2)) \implies \dots$$

$$(3.1) \phi(h_1) = h_1N = h_2N = \phi(h_2) \blacksquare \phi(h_1) = \phi(h_2)$$

$$(4) ((h_1, h_2 \in H) \wedge (h_1 = h_2)) \implies (\phi(h_1) = \phi(h_2)) \blacksquare \forall_{h_1, h_2 \in H} \left( (h_1 = h_2) \implies (\phi(h_1) = \phi(h_2)) \right) \blacksquare \text{Func}[\phi, H, (HN)/N]$$

$$(5) (h_1, h_2 \in H) \implies \dots$$

$$(5.1) \phi(h_1 * h_2) = (h_1 * h_2)N = (h_1N) \bar{*} (h_2N) = \phi(h_1) \bar{*} \phi(h_2) \blacksquare \phi(h_1 * h_2) = \phi(h_1) \bar{*} \phi(h_2)$$

$$(6) (h_1, h_2 \in H) \implies (\phi(h_1 * h_2) = \phi(h_1) \bar{*} \phi(h_2)) \blacksquare \forall_{h_1, h_2 \in H} (\phi(h_1 * h_2) = \phi(h_1) \bar{*} \phi(h_2))$$

$$(7) (\text{Func}[\phi, H, (HN)/N]) \wedge \left( \forall_{h_1, h_2 \in H} (\phi(h_1 * h_2) = \phi(h_1) \bar{*} \phi(h_2)) \right) \blacksquare \text{Homomorphism}[\phi, H, *, (HN)/N, \bar{*}]$$

$$(8) \ker_\phi = \{ h \in H \mid \phi(h) = e_{(HN)/N} \} = \{ h \in H \mid hN = N \} = \{ h \in H \mid h \in N \} = \{ h \mid (h \in H) \wedge (h \in N) \} = H \cap N \blacksquare \ker_\phi = H \cap N$$

$$(9) \text{im}_\phi = \{ \phi(h) \mid h \in H \} = \{ hN \mid h \in H \} = (HN)/N \blacksquare \text{im}_\phi = (HN)/N$$

$$(10) (\text{FirstMapThm}) \wedge (\text{Homomorphism}[\phi, H, *, (HN)/N, \bar{*}]) \blacksquare \text{Isomorphic}[H/\ker_\phi, \bar{*}, \text{im}_\phi, \bar{*}]$$

$$(11) (\ker_\phi = H \cap N) \wedge (\text{im}_\phi = (HN)/N) \wedge (\text{Isomorphic}[H/\ker_\phi, \bar{*}, \text{im}_\phi, \bar{*}]) \blacksquare \text{Isomorphic}[H/(H \cap N), \bar{*}, (HN)/N, \bar{*}]$$

$$\text{ThirdMap}[\phi, K, H, G, *] := \left( \begin{array}{c} \left( \phi = \{ \langle gK, gH \rangle \in ((G/K) \times (G/H)) \mid g \in G \} \right) \\ ( \text{NormalSubgroup}[K, G, *]) \wedge (\text{NormalSubgroup}[H, G, *]) \wedge (\text{Subgroup}[K, H, *]) \end{array} \right) \wedge$$

$$\text{ThirdIsoThm} := \left( \begin{array}{c} ((\text{NormalSubgroup}[K, G, *]) \wedge (\text{NormalSubgroup}[H, G, *]) \wedge (\text{Subgroup}[K, H, *])) \implies \\ (\text{Isomorphic}[(G/K)/(H/K), \bar{*}, G/H, \bar{*}]) \end{array} \right)$$

$$(1) \text{ ThirdMap}[\phi, K, H, G, *] \blacksquare \phi = \{ \langle gK, gH \rangle \in ((G/K) \times (G/H)) \mid g \in G \}$$

$$(2) ((g_1K, g_2K \in (G/K)) \wedge (g_1K = g_2K)) \implies \dots$$

$$(2.1) g_1K = g_2K \blacksquare (g_2)^{-1}g_1K = K \blacksquare (g_2)^{-1}g_1 \in K$$

$$(2.2) (K \subseteq H) \wedge ((g_2)^{-1}g_1 \in K) \blacksquare (g_2)^{-1}g_1 \in H$$

$$(2.3) (g_2)^{-1}g_1 \in H \blacksquare g_1H = g_2H \blacksquare \phi(g_1K) = g_1H = g_2H = \phi(g_2K) \blacksquare \phi(g_1K) = \phi(g_2K)$$

$$(3) ((g_1K, g_2K \in (G/K)) \wedge (g_1K = g_2K)) \implies (\phi(g_1K) = \phi(g_2K)) \blacksquare \forall_{g_1K, g_2K \in (G/K)} ((g_1K = g_2K) \implies (\phi(g_1K) = \phi(g_2K))) \dots$$

$$(4) \dots \text{Func}[\phi, G/K, G/H]$$

$$(5) (g_1K, g_2K \in (G/K)) \implies \dots$$

$$(5.1) \phi(g_1K \bar{*} g_2K) = \phi((g_1 * g_2)K) = (g_1 * g_2)H = (g_1H) \bar{*} (g_2H) = \phi(g_1K) \bar{*} \phi(g_2K) \blacksquare \phi(g_1K \bar{*} g_2K) = \phi(g_1K) \bar{*} \phi(g_2K)$$

$$(6) (g_1K, g_2K \in (G/K)) \implies (\phi(g_1K \bar{*} g_2K) = \phi(g_1K) \bar{*} \phi(g_2K)) \blacksquare \forall_{g_1K, g_2K \in (G/K)} (\phi(g_1K \bar{*} g_2K) = \phi(g_1K) \bar{*} \phi(g_2K))$$

$$(7) (\text{Func}[\phi, G/K, G/H]) \wedge \left( \forall_{g_1K, g_2K \in (G/K)} (\phi(g_1K \bar{*} g_2K) = \phi(g_1K) \bar{*} \phi(g_2K)) \right) \blacksquare \text{Homomorphism}[\phi, G/K, \bar{*}, G/H, \bar{*}]$$

$$(8) \ker_\phi = \{ gK \in (G/K) \mid \phi(gK) = e_{G/H} \} = \{ gK \in (G/K) \mid gH = H \} = \{ gK \in (G/K) \mid g \in H \} = H/K \blacksquare \ker_\phi = H/K$$

$$(9) (y \in (G/H)) \implies \dots$$

$$(9.1) \exists_{g \in G} (y = gH)$$

$$(9.2) g \in G \blacksquare gK \in (G/K)$$

$$(9.3) \phi(gK) = gH = y \blacksquare y = \phi(gK)$$

$$(9.4) (gK \in (G/K)) \wedge (y = \phi(gK)) \blacksquare \exists_{gK \in (G/K)} (y = \phi(gK))$$

$$(10) (y \in (G/H)) \implies \left( \exists_{gK \in (G/K)} (y = \phi(gK)) \right) \blacksquare \forall_{y \in (G/H)} \exists_{gK \in (G/K)} (y = \phi(gK)) \blacksquare \text{Surj}[\phi, G/K, G/H]$$

$$(11) (\text{SurjEquiv}) \wedge (\text{Surj}[\phi, G/K, G/H]) \blacksquare \text{im}_\phi = G/H$$

$$(12) (\text{FirstMapThm}) \wedge (\text{Homomorphism}[\phi, G/K, \bar{*}, G/H, \bar{*}]) \blacksquare \text{Isomorphic}[(G/K)/\ker_\phi, \bar{*}, \text{im}_\phi, \bar{*}]$$







# Chapter 3

## Linear Algebra

### 3.1 Matrix Operations and Special Matrices

$Matrix[A, m, n] := [a_{i,j}]_{m \times n} := m \text{ rows, } n \text{ columns of real numbers}$

$\mathcal{M}_{m,n} := \{A : Matrix[A, m, n]\}$

$O_{m,n} := (Matrix[O, m, n]) \wedge (a_{i,j} = 0)$

$Square[A, n] := Matrix[A, n, n]$

$UpperTriangular[A] := (Square[A]) \wedge (i > j \implies a_{i,j} = 0)$

$LowerTriangular[A] := (Square[A]) \wedge (i < j \implies a_{i,j} = 0)$

$Diagonal[A, n] := (Square[A, n]) \wedge (i \neq j \implies a_{i,j} = 0)$

$Scalar[A, n, k] := (Diagonal[A, n]) \wedge (a_{i,i} = k)$

$I_n := Scalar[I, n, 1]$

$+(A, B) := ((Matrix[A, m, n]) \wedge (Matrix[B, m, n])) \implies (A + B = [a_{i,j} + b_{i,j}]_{m \times n})$

$*(r, A) := ((r \in \mathbb{R}) \wedge (Matrix[A, m, n])) \implies (r * A = [ra_{i,j}]_{m \times n})$

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

$^T[A] := (Matrix[A, m, n]) \implies (A^T = [a_{j,i}]_{n \times m})$

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

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

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

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

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

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

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

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

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

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

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

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

$$(2) \quad \text{TODO} = A$$

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

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

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

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

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

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

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

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

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

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

$$(1) \quad \text{TODO}$$

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

$$(1) \quad \text{TODO}$$

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

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

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

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

$$(1) \quad \text{TODO}$$

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

$$(1) \quad \text{TODO}$$

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

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

$$\text{Sym}[A] := A = A^T$$

$$\text{SkewSym}[A] := A = -A^T$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### 3.2 Elementary Matrices on Invertibility and Systems of Linear Equations

$$Sys[A, B] := (Matrix[A, m, n]) \wedge (Matrix[B, m, 1])$$

$$Sol[X, A, B] := (Sys[A, B]) \wedge (Matrix[X, n, 1]) \wedge (A * X = B)$$

$$ConsistentSys[A, B] := (Sys[A, B]) \wedge \exists_X (Sol[X, A, B])$$

$$TrivSol[X, A] := (Sol[X, A, O]) \wedge (X = O)$$

$$NonTrivSol[X, A] := (Sol[X, A, O]) \wedge (X \neq O)$$

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

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

$$(2) \quad TrivSol[u_0, A]$$

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

$$(4) \quad (TrivSol[\vec{X}, A]) \implies (TrivSol[LC(\vec{X}), A])$$

$$ElemMat[E] := (E = Swap[I_n, i, j]) \vee (Scale_*(I_n, i, c)) \vee (Combine_*(I_n, i, c, j))$$

$$ElemMatProd[E^*] := \exists_{\langle E \rangle} \left( \forall_{E_i \in E^*} (ElemMat[E_i]) \wedge \left( E^* = \prod_{E_i \in E^*} (E_i) \right) \right)$$

$$RowEquiv[A, B] := \exists_{E^*} ((ElemMatProd[E^*]) \wedge (B = E^* * A))$$

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

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

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

$$(1) \quad TODO$$

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

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

---


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


---

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


---

$$(3.1) \quad A * Y = B$$


---

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


---

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


---

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


---

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


---

$$(6.1) \quad C * Z = D$$


---

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


---

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


---

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


---

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


---

$$(1) \quad \text{Set } B = D = O$$


---

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


---

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


---

$$(1) \quad \text{Hit } A \text{ with } ElemMat\text{'s until it becomes } B$$


---

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


---

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


---

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


---

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


---

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


---

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


---

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


---

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


---

$$(1) \quad (Invertible[A]) \implies \dots$$


---

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


---

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


---

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


---

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


---

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


---

$$(1.6) \quad RowEquiv[A, I_n]$$


---

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


---

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


---

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


---

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


---

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


---

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


---

$$RowEquivIf f TrivSol := \forall_{A \in \mathcal{M}} \left( (RowEquiv[A, I_n]) \iff \left( \forall_X ((X = O) \iff (Sol[X, A, O])) \right) \right)$$


---

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


---

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


---

$$\begin{aligned}
(1.2) \quad & (Sol[X, A, O]) \implies \dots \\
(1.2.1) \quad & A * X = O \quad \blacksquare \quad X = A^{-1} * O = O \quad \blacksquare \quad X = O \\
(1.3) \quad & (Sol[X, A, O]) \implies (X = O) \\
(1.4) \quad & (X = O) \implies (Sol[X, A, O]) \\
(1.5) \quad & (X = O) \iff (Sol[X, A, O]) \quad \blacksquare \quad \forall_X ((X = O) \iff (Sol[X, A, O]))
\end{aligned}$$

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

$$(3) \quad \left( \forall_X ((X = O) \iff (Sol[X, A, O])) \right) \implies \dots$$

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

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

$$(3.3) \quad (B \neq I_n) \implies \dots$$

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

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

$$(3.3.3) \quad (Y \neq X) \wedge (Y = X) \quad \blacksquare \quad \perp$$

$$(3.4) \quad (B \neq I_n) \implies \perp \quad \blacksquare \quad B = I_n$$

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

$$(4) \quad \left( \forall_X ((X = O) \iff (Sol[X, A, O])) \right) \implies (RowEquiv[A, I_n])$$

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

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

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

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

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

$$(2) \quad \left( \forall_{B \in \mathcal{M}} \exists!_{X \in \mathcal{M}} (Sol[X, A, B]) \right) \implies \dots$$

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

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

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

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

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

### 3.3 Vector Spaces

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(2) \quad (r * v = O) \implies \dots$$

$$(2.1) \quad (r \neq 0) \implies \dots$$

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

$$(2.1.2) \quad ZeroVectorGenRight \quad \blacksquare \quad O = r^{-1} * O = r^{-1} * (r * v) = (r^{-1}r) * v = 1 * v = v \quad \blacksquare \quad O = v$$

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

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

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

### 3.4 Subspaces and Special Subspaces

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

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

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

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

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

$$(1.3) \quad (\emptyset \neq S) \wedge (S \subseteq V) \quad \blacksquare \quad \emptyset \neq S \subseteq V$$

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

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

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

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

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

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

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

$$(3.1.3) \quad u, v \in V \quad \blacksquare \quad u + v = v + u$$

$$(3.1.4) \quad u, v, w \in V \quad \blacksquare \quad (u + v) + w = u + (v + w)$$

$$(3.1.5) \quad u \in V \quad \blacksquare \quad u + O = u$$

$$(3.1.6) \quad (AddInvGen) \wedge (u \in S) \quad \blacksquare \quad (-1) * u = -u \in S$$

$$(3.1.7) \quad u \in V \quad \blacksquare \quad \alpha * (\beta * u) = (\alpha\beta) * u$$

$$(3.1.8) \quad u \in V \quad \blacksquare \quad 1 * u = u$$

$$(3.1.9) \quad u, v \in V \quad \blacksquare \quad \alpha * (u + v) = (\alpha * u) + (\alpha * v)$$

$$(3.1.10) \quad u \in V \quad \blacksquare \quad (\alpha + \beta) * u = (\alpha * u) + (\beta * u)$$

$$(4) \quad ((\emptyset \neq S) \wedge (\forall_{r, s \in S} (r + s \in S)) \wedge (\forall_{\alpha \in \mathbb{R}} \forall_{s \in S} (\alpha * s \in S))) \implies (Subspace[S, V, +, *])$$

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

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

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

$$(1) \quad (\text{Subspace}[A, V, +, *]) \wedge (\text{Subspace}[B, V, +, *]) \quad \blacksquare \quad (O \in A) \wedge (O \in B)$$

$$(2) \quad (\text{SetSum}[A + B, A, B, V, +, *]) \wedge (O \in A) \wedge (O \in B) \quad \blacksquare \quad O = O + O \in A + B \quad \blacksquare \quad \emptyset \neq A + B$$

$$(3) \quad (v \in A + B) \implies \dots$$

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

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

$$(3.3) \quad \text{VectorSpace}[V, +, *] \quad \blacksquare \quad v = a + b \in V$$

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

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

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

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

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

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

$$(7) \quad (u, v \in A + B) \implies (u + v \in A + B) \quad \blacksquare \quad \forall_{u,v \in A+B} (u + v \in A + B)$$

$$(8) \quad ((r \in \mathbb{R}) \wedge (v \in A + B)) \implies \dots$$

$$(8.1) \quad \exists_{a \in A} \exists_{b \in B} (v = a + b)$$

$$(8.2) \quad r * v = r * (a + b) = r * a + r * b$$

$$(8.3) \quad (r * a \in A) \wedge (r * b \in B) \quad \blacksquare \quad r * v \in A + B$$

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

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

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

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

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

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

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

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

$$(2) \quad ((\text{Subspace}[C, V, +, *]) \wedge (A, B \subseteq C)) \implies \dots$$

$$(2.1) \quad (s \in A + B) \implies \dots$$

$$(2.1.1) \quad \exists_{a \in A} \exists_{b \in B} (s = a + b)$$

$$(2.1.2) \quad (A, B \subseteq C) \quad \blacksquare \quad a, b \in C$$

$$(2.1.3) \quad (\text{VectorSpace}[C, V, +, *]) \wedge (a, b \in C) \quad \blacksquare \quad s = a + b \in C$$

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

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

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

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

$$(1) \quad (\text{DirSum}[A \oplus B, A, B, V, +, *]) \implies \dots$$

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

$$(1.2) \quad (SubSum[A \oplus B, A, B, V, +, *]) \wedge (O \in A) \wedge (O \in B) \quad \blacksquare \quad O = O + O \in A \oplus B$$

$$(1.3) \quad (DirSum[A \oplus B, A, B, V, +, *]) \wedge (O \in A \oplus B) \quad \blacksquare \quad \exists!_{\langle a, b \rangle \in A \times B} (O = a + b)$$

$$(2) \quad (DirSum[A \oplus B, A, B, V, +, *]) \implies \left( \exists!_{\langle a, b \rangle \in A \times B} (O = a + b) \right)$$

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

$$(3.1) \quad (s \in A \oplus B) \implies \dots$$

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

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

$$(3.1.2.1) \quad O = s - s = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$$

$$(3.1.2.2) \quad (Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *]) \quad \blacksquare \quad (a_1 - a_2 \in A) \wedge (b_1 - b_2 \in B)$$

$$(3.1.2.3) \quad ((a_1 - a_2 \neq O) \vee (b_1 - b_2 \neq O)) \implies \left( \neg \exists!_{\langle a, b \rangle \in A \times B} (O = a + b) \right) \implies \perp$$

$$(3.1.2.4) \quad (a_1 - a_2 = O) \wedge (b_1 - b_2 = O) \quad \blacksquare \quad \langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle$$

$$(3.1.3) \quad ((s = a_1 + b_1) \wedge (s = a_2 + b_2)) \implies \langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle$$

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

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

$$(3.2) \quad (s \in A + B) \implies \exists!_{\langle a, b \rangle \in A \times B} (s = a + b) \quad \blacksquare \quad \forall_{s \in A + B} \exists!_{\langle a, b \rangle \in A \times B} (s = a + b) \quad \blacksquare \quad DirSum[A \oplus B, A, B, V, +, *]$$

$$(4) \quad \left( \exists!_{\langle a, b \rangle \in A \times B} (O = a + b) \right) \implies (DirSum[A \oplus B, A, B, V, +, *])$$

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

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

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

$$(1.1) \quad (v \in A \cap B) \implies \dots$$

$$(1.1.1) \quad (v \in A \cap B) \wedge (VectorSpace[B, +, *]) \quad \blacksquare \quad (v \in A) \wedge (v \in B) \quad \blacksquare \quad (v \in A) \wedge (-v \in B)$$

$$(1.1.2) \quad (v \in A) \wedge (-v \in B) \quad \blacksquare \quad v + (-v) = O \in A + B$$

$$(1.1.3) \quad DirSum[A \oplus B, A, B, V, +, *] \quad \blacksquare \quad \exists!_{\langle a, b \rangle \in A \times B} (O = a + b)$$

$$(1.1.4) \quad (v \neq O) \implies \left( \neg \exists!_{\langle a, b \rangle \in A \times B} (O = a + b) \right) \implies \perp \quad \blacksquare \quad v = O$$

$$(1.2) \quad (v \in A \cap B) \implies (v = O) \quad \blacksquare \quad A + B \subseteq \{O\}$$

$$(1.3) \quad (v = O) \implies \dots$$

$$(1.3.1) \quad (Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *]) \quad \blacksquare \quad (O \in A) \wedge (O \in B) \quad \blacksquare \quad v = O \in A \cup B$$

$$(1.4) \quad (v = O) \implies (v \in A \cap B) \quad \blacksquare \quad \{O\} \subseteq A \cap B$$

$$(1.5) \quad (A + B \subseteq \{O\}) \wedge (\{O\} \subseteq A \cap B) \quad \blacksquare \quad A \cap B = \{O\}$$

$$(2) \quad (DirSum[A \oplus B, A, B, V, +, *]) \implies (A \cap B = \{O\})$$

$$(3) \quad (A \cap B = \{O\}) \implies \dots$$

$$(3.1) \quad (O \in A) \wedge (O \in B) \wedge (O = O + O \in A + B) \quad \blacksquare \quad \exists_{\langle a, b \rangle \in A \times B} (O = a + b)$$

$$(3.2) \quad ((\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \in A \times B) \wedge (O = a_1 + b_1) \wedge (O = a_2 + b_2)) \implies \dots$$

$$(3.2.1) \quad (O = a_1 + b_1) \wedge (O = a_2 + b_2) \quad \blacksquare \quad (a_1 = -b_1) \wedge (a_2 = -b_2)$$

$$(3.2.2) \quad VectorSpace[B, +, *] \quad \blacksquare \quad -b_1, -b_2 \in B$$

$$(3.2.3) \quad (a_1 \in A) \wedge (a_1 = -b_1 \in B) \quad \blacksquare \quad a_1 \in A \cap B \quad \blacksquare \quad a_1 = O \quad \blacksquare \quad a_1 = b_1 = O$$

$$(3.2.4) \quad (a_2 \in A) \wedge (a_2 = -b_2 \in B) \quad \blacksquare \quad a_2 \in A \cap B \quad \blacksquare \quad a_2 = O \quad \blacksquare \quad a_2 = b_2 = O$$

$$(3.2.5) \quad \langle a_1, b_1 \rangle = \langle O, O \rangle = \langle a_2, b_2 \rangle$$

$$(3.3) \quad ((\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \in A \times B) \wedge (O = a_1 + b_1) \wedge (O = a_2 + b_2)) \implies (\langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle)$$

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

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



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

$$(4) \quad (A \cap B = \{O\}) \implies (DirSum[A \oplus B, A, B, V, +, *])$$

$$(5) \quad (DirSum[A \oplus B, A, B, V, +, *]) \iff (A \cap B = \{O\})$$

$$NullSpace[N, A, m, n] := (Matrix[A, m, n]) \wedge (N = \{x \in \mathbb{R}^n \mid A * x = O\})$$

$$RowSpace[R, A, m, n] := (Matrix[A, m, n]) \wedge (R = \{x^T * A \in \mathbb{R}^n \mid x \in \mathbb{R}^m\})$$

$$ColSpace[C, A, m, n] := (Matrix[A, m, n]) \wedge (C = \{A * x \in \mathbb{R}^m \mid x \in \mathbb{R}^n\})$$

$$NullSubspace := (NullSpace[N, A, m, n]) \implies (Subspace[N, \mathbb{R}^n, +, *])$$

(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

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

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

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

(1)  $(S = \emptyset) \implies \dots$

$$(1.1) \quad LinSpan[S', S, V, +, *] \quad \blacksquare \quad S' = \{O\}$$

$$(1.2) \quad Subspace[\{O\}, V, +, *] \quad \blacksquare \quad Subspace[S', V, +, *]$$

$$(1.3) \quad S = \emptyset \subseteq \{O\} = S' \quad \blacksquare \quad S \subseteq S'$$

$$(1.4) \quad (Subspace[S', V, +, *]) \wedge (S \subseteq S')$$

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

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

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

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

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

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

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

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

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

$$(3.4.4) \quad \left( a + b = \sum_{i=1}^n ((k_{ai} + k_{bi}) * s_i) \right) \wedge (\langle k_{ai} + k_{bi} \mid i \in \mathbb{N}_{1,n} \rangle \in \mathbb{R}^n) \quad \dots$$

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

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

(3.6)  $(r \in \mathbb{R}) \wedge (u \in S') \implies \dots$

$$(3.6.1) \quad \exists_{K \in \mathbb{R}^n} (LinComb[u, S, K, V, +, *]) \quad \blacksquare \quad u = \sum_{i=1}^n (k_i * s_i)$$

$$(3.6.2) \quad r * u = r * \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^n (r * (k_i * s_i)) = \sum_{i=1}^n (rk_i) * s_i \quad \blacksquare \quad r * u = \sum_{i=1}^n (rk_i) * s_i$$

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

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

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

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

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

$$(3.9) \quad (s_i \in S) \implies \dots$$

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

$$(3.9.2) \quad \exists_{K \in \mathbb{R}^n} (LinComb[s_j, S, K, V, +, *]) \quad \blacksquare \quad s_j \in S'$$

$$(3.10) \quad (s_i \in S) \implies (s_i \in S') \quad \blacksquare \quad S \subseteq S'$$

$$(3.11) \quad (Subspace[S', V, +, *]) \wedge (S \subseteq S')$$

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

$$(5) \quad \left( (S = \emptyset) \implies ((Subspace[S', V, +, *]) \wedge (S \subseteq S')) \right) \wedge \left( (S \neq \emptyset) \implies ((Subspace[S', V, +, *]) \wedge (S \subseteq S')) \right) \dots$$

$$(6) \quad \dots (Subspace[S', V, +, *]) \wedge (S \subseteq S')$$

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

$$(1) \quad (s' \in S') \implies \dots$$

$$(1.1) \quad \exists_{K \in \mathbb{R}^n} (LinComb[s', S, K, V, +, *]) \quad \blacksquare \quad s' = \sum_{i=1}^n (k_i * s_i)$$

$$(1.2) \quad (S \subseteq W) \wedge (VectorSpace[W, V, +, *]) \quad \blacksquare \quad s' = \sum_{i=1}^n (k_i * s_i) \in W \quad \blacksquare \quad s' \in W$$

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

$$Spans[S, V, +, *] := LinSpan[V, S, V, +, *]$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(1.2) \quad A \subseteq B \quad \blacksquare \quad \forall_{j \in \mathbb{N}_{1,n}} (a_j = b_j) \quad \blacksquare \quad \sum_{i=1}^n (k_i * a_i) = \sum_{j=1}^m (l_j * b_j)$$

$$(1.3) \quad \text{LinComb}[O, A, K, V, +, *] \quad \blacksquare \quad O = \sum_{i=1}^n (k_i * a_i) = \sum_{j=1}^m (l_j * b_j) \quad \blacksquare \quad \text{LinComb}[O, B, L, V, +, *]$$

$$(1.4) \quad (\text{LinInd}[B, V, +, *]) \wedge (\text{LinComb}[O, B, L, V, +, *]) \quad \blacksquare \quad L = \{0\}^m \quad \blacksquare \quad K = \{0\}^n$$

$$(2) \quad ((K \in \mathbb{R}^n) \wedge (\text{LinComb}[O, A, K, V, +, *])) \implies (K = \{0\}^n) \quad \blacksquare \quad \text{LinInd}[A, V, +, *]$$

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

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

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

$$(3) \quad A \subseteq B \quad \blacksquare \quad \forall_{j \in \mathbb{N}_{1,n}} (a_j = b_j) \quad \blacksquare \quad \sum_{i=1}^n (k_i * a_i) = \sum_{j=1}^m (l_j * b_j)$$

$$(4) \quad \text{LinComb}[O, A, K, V, +, *] \quad \blacksquare \quad \text{LinComb}[O, B, L, V, +, *]$$

$$(5) \quad K \neq \{0\}^n \quad \blacksquare \quad L \neq \{0\}^m$$

$$(6) \quad \exists_L ((\text{LinComb}[O, B, L, V, +, *]) \wedge (L \neq \{0\}^m)) \quad \blacksquare \quad \neg \text{LinInd}[B, V, +, *]$$

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

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

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

$$(3) \quad \dots \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^j (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j \quad \blacksquare \quad \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j$$

$$(4) \quad (\text{LinComb}[O, S, K, V, +, *]) \wedge \left( \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j \right) \quad \blacksquare \quad O = \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j$$

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

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

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

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

$$(2) \quad \forall_{u \in P} \left( \left( \exists_{K_1} (\text{LinComb}[u, S, K_1, V, +, *]) \right) \implies \left( \exists_{K_2} (\text{LinComb}[u, S \setminus \{s_j\}, K_2, V, +, *]) \right) \right) \quad \blacksquare \quad \text{LinSpan}[P, S \setminus \{s_j\}, V, +, *]$$

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

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

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

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

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

$$(3.2) \quad \text{LinComb}[s_j, S \setminus \{s_j\}, K, V, +, *] \quad \blacksquare \quad \dots \quad \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j = \sum_{i=1}^{j-1} (k_i * s_i) + - \sum_{i=1}^{j-1} (k_i * s_i) = O \quad \dots$$

$$(3.3) \quad \dots \text{LinComb}[O, S, L, V, +, *]$$

$$(3.4) \quad (\text{LinComb}[O, S, L, V, +, *]) \wedge (L \neq \{0\}^n) \quad \blacksquare \quad \exists_{L \in \mathbb{R}^n} ((\text{LinComb}[O, S, L, V, +, *]) \wedge (L \neq \{0\}^n)) \quad \blacksquare \quad (\neg \text{LinInd}[S, V, +, *])$$

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

---


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


---

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


---

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


---

$$(1) \quad (\neg LinInd[W, V, +, *]) \implies \dots$$


---

$$(1.1) \quad \exists_{j \in W} (LinComb[j, W \setminus \{j\}, +, *]) \quad \blacksquare \quad \neg LinInd[W, U, +, *]$$


---

$$(1.2) \quad (LinInd[W, U, +, *]) \wedge (\neg LinInd[W, V, +, *]) \quad \blacksquare \quad \perp$$


---

$$(2) \quad (\neg LinInd[W, V, +, *]) \implies \perp \quad \blacksquare \quad LinInd[W, V, +, *]$$


---

### 3.6 Bases and Dimensions

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

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


---

$$(1) \quad (Basis[S, V, +, *]) \implies \dots$$


---

$$(1.1) \quad (v \in V) \implies \dots$$


---

$$(1.1.1) \quad Basis[S, V, +, *] \quad \blacksquare \quad Spans[V, S, +, *] \quad \blacksquare \quad \exists_{K \in \mathbb{R}^n} (LinComb[v, S, K, V, +, *])$$


---

$$(1.1.2) \quad ((K_1, K_2 \in \mathbb{R}^n) \wedge (LinComb[v, S, K_1, V, +, *]) \wedge (LinComb[v, S, K_2, V, +, *])) \implies \dots$$


---

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


---

$$(1.1.2.2) \quad 0 = v - v = \sum(k_{1i} * s_i) - \sum(k_{2i} * s_i) = \sum((k_{1i} - k_{2i}) * s_i)$$


---

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


---

$$(1.1.2.4) \quad (LinInd[S, V, +, *]) \wedge (LinComb[0, S, L, V, +, *]) \quad \blacksquare \quad L = \{0\}^n \quad \blacksquare \quad K_2 = K_1$$


---

$$(1.1.3) \quad ((K_1, K_2 \in \mathbb{R}^n) \wedge (LinComb[v, S, K_1, V, +, *]) \wedge (LinComb[v, S, K_2, V, +, *])) \implies (K_1 = K_2)$$


---

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


---

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


---

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


---

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


---

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


---

$$(3.1) \quad \forall_{v \in V} \exists!_{K \in \mathbb{R}^n} (LinComb[v, S, K, V, +, *]) \quad \blacksquare \quad \forall_{v \in V} \exists_{K \in \mathbb{R}^n} (LinComb[v, S, K, V, +, *]) \quad \blacksquare \quad Spans[S, V, +, *]$$


---

$$(3.2) \quad 0 \in V \quad \blacksquare \quad \exists!_{K \in \mathbb{R}^n} (LinComb[0, S, K, V, +, *])$$


---

$$(3.3) \quad (K \neq \{0\}^n) \implies (\neg \exists!_{K \in \mathbb{R}^n} (LinComb[0, S, K, V, +, *])) \implies \perp \quad \blacksquare \quad K = \{0\}^n$$


---

$$(3.4) \quad (\exists!_{K \in \mathbb{R}^n} (LinComb[0, S, K, V, +, *])) \wedge (K = \{0\}^n) \quad \blacksquare \quad LinInd[S, V, +, *]$$


---

$$(3.5) \quad (Spans[S, V, +, *]) \wedge (LinInd[S, V, +, *]) \quad \blacksquare \quad Basis[S, V, +, *]$$


---

$$(4) \quad (\forall_{v \in V} \exists!_{K \in \mathbb{R}^n} (LinComb[v, S, K, V, +, *])) \implies (Basis[S, V, +, *])$$


---

$$SpanReduceBasis := \forall_{S, V} \left( (Spans[S, V, +, *]) \implies \left( \exists_B ((B \subseteq S) \wedge (Basis[B, V, +, *])) \right) \right)$$


---

$$(1) \quad LinDepPropCorollary \quad \blacksquare \quad \exists_B ((B \subseteq S) \wedge (LinInd[B, V, +, *]) \wedge (Spans[B, V, +, *])) \quad \blacksquare \quad \exists_B ((B \subseteq S) \wedge (Basis[B, V, +, *]))$$


---

$$(2) \quad \text{TODO - formalize removing latter entries first}$$


---

$$FinDimBasis := \forall_V \left( (FinDim[V, +, *]) \implies (\exists_B (Basis[B, V, +, *])) \right)$$


---

$$(1) \quad FinDim[V, +, *] \quad \blacksquare \quad \exists_{S \in V^n} (Spans[S, V, +, *])$$


---

$$(2) \quad (SpanReduceBasis) \wedge (Spans[S, V, +, *]) \quad \blacksquare \quad \exists_B (Basis[B, V, +, *])$$


---

$$LinIndExpandBasis := \forall_{L, V} \left( (LinInd[L, V, +, *]) \implies \left( \exists_B ((L \subseteq B) \wedge (Basis[B, V, +, *])) \right) \right)$$

- 
- (1)  $FinDimBasis \dashv \exists_C (Basis[C, V, +, *])$
- 
- (2)  $S := L \cup C$
- 
- (3)  $Basis[C, V, +, *] \dashv Spans[C, V, +, *] \dashv Spans[S, V, +, *]$
- 
- (4)  $SpanReduceBasis \dashv \left( \exists_B ((B \subseteq S) \wedge (Basis[B, V, +, *])) \right) \wedge (L \subseteq B)$
- 

$$SpanLinIndLength := \forall_{S,T,V} \left( ((Span[S, V, +, *]) \wedge (LinInd[T, V, +, *])) \implies (|T| \leq |S|) \right)$$


---

- (1)  $((Span[S, V, +, *]) \wedge (|T| > |S|)) \implies \dots$
- 
- (1.1)  $Span[S, V, +, *] \dashv \forall_{i \in \mathbb{N}_{1, |H|}} \exists_{K_i \mathbb{R}^{|S|}} (LinComb[t_i, S, K_i V, +, *])$
- 
- (1.2)  $|H| > |S| \dashv \exists_{L \in \mathbb{R}^{|H|-1}} (LinComb[t_{|H|}, T \setminus \{t_{|H|}\}, L, V, +, *])$
- 
- (1.3)  $L = -1 * K \dashv (\sum (K + L) = O) \wedge (K + L \neq \{0\}^{|T|}) \dashv \neg LinInd[T, V, +, *]$
- 
- (1.4) TODO - tidy up
- 
- (2)  $((Span[S, V, +, *]) \wedge (|T| > |S|)) \implies (\neg LinInd[T, V, +, *]) \dashv ((Span[S, V, +, *]) \wedge (LinInd[T, V, +, *])) \implies (|T| \leq |S|)$
- 

$$BasisLength := \forall_{S,T,V} \left( ((Basis[S, V, +, *]) \wedge (Basis[T, V, +, *])) \implies (|T| = |S|) \right)$$


---

- (1)  $(Span[T, V, +, *]) \wedge (LinInd[S, V, +, *]) \dashv |S| \leq |T|$
- 
- (2)  $(Span[S, V, +, *]) \wedge (LinInd[T, V, +, *]) \dashv |T| \leq |S|$
- 
- (3)  $(|S| \leq |T|) \wedge (|T| \leq |S|) \dashv |T| = |S|$
- 

$$Dim[d, V, +, *] := ((V = \{O\}) \implies (d = 0)) \wedge ((V \neq \{O\}) \implies ((\exists_B (Basis[B, V, +, *])) \wedge (d = |B|)))$$


---

$$LinIndLengthDim := \forall_{U,V} \left( ((LinInd[U, V, +, *]) \wedge (Dim[|U|, V, +, *])) \implies (Basis[U, V, +, *]) \right)$$


---

- (1)  $(LinIndExpandBasis) \wedge (LinInd[U, V, +, *]) \dashv \exists_B ((U \subseteq B) \wedge (Basis[B, V, +, *]))$
- 
- (2)  $(BasisLength) \wedge (Dim[|U|, V, +, *]) \wedge (Basis[B, V, +, *]) \dashv |B| = |U| \dashv B = U \dashv Basis[U, V, +, *]$
- 

$$SpanLengthDim := \forall_{U,V} \left( ((Spans[U, V, +, *]) \wedge (Dim[|U|, V, +, *])) \implies (Basis[U, V, +, *]) \right)$$


---

- (1)  $(SpanReduceBasis) \wedge (Spans[U, V, +, *]) \dashv \exists_B ((B \subseteq U) \wedge (Basis[B, V, +, *]))$
- 
- (2)  $(BasisLength) \wedge (Dim[|U|, V, +, *]) \wedge (Basis[B, V, +, *]) \dashv |B| = |U| \dashv B = U \dashv Basis[U, V, +, *]$
- 

$$LinDepLengthDim := \forall_{U,V} \left( ((U \subseteq V) \wedge (|U| > Dim[V])) \implies (\neg LinInd[U, V, +, *]) \right)$$


---

- (1) Contrapositive of  $BasisLinearIndCard$
- 
- (2) TODO - cleanup
- 

$$NonSpanLengthDim := \forall_{U,V} \left( ((U \subseteq V) \wedge (|U| < Dim[V])) \implies (\neg Spans[U, V, +, *]) \right)$$


---

- (1) Suppose  $Spans[U, V, +, *]$ ,  $B = SpanReduceBasis[U]$  to form a basis,  $(|B| \leq |U| < Dim[V]) \wedge |B| = Dim[V] \dashv \perp$
- 
- (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

---

$$\text{RankInv} := \forall_A \left( (\text{Matrix}[A, m, n]) \implies ((\text{Rank}[A] = n) \iff (\text{Inv}[A])) \right)$$


---

(1) TODO

---

$$\text{RankNonTrivialSol} := \left( \exists_X ((A * X = O) \wedge (X \neq O)) \right) \iff (\text{Rank}[A] < n)$$


---

(1) TODO

---

$$\text{RankUniqueSol} := (\forall_{B \in \mathcal{M}} \exists!_{X \in \mathcal{M}} (\text{Sol}[X, A, B])) \iff (\text{Rank}[A] = n)$$


---

(1) TODO

---

$$\text{SquareTheorems}_8 := \forall_{A \in \mathcal{M}} \left( \begin{array}{l} (\text{Invertible}[A]) \iff \\ (\text{RowEquiv}[A, I_n]) \iff \\ \left( \forall_X ((X = O) \iff (\text{Sol}[X, A, O])) \right) \iff \\ (\forall_{B \in \mathcal{M}} \exists!_{X \in \mathcal{M}} (\text{Sol}[X, A, B])) \iff \\ (\text{Rank}[A] = n) \iff \\ (\text{Nullity}[A] = 0) \iff \\ (\text{The rows form a linearly independent set of vectors (to get full rank)}) \iff \\ (\text{The columns form a linearly independent set of vectors (to get full rank)}) \iff \end{array} \right)$$


---

### 3.8 Linear Transformations

$$\text{LinTrans}[L, V, +_v, *_v, W, +_w, *_w] := \left( \begin{array}{l} (\text{Function}[f, V, W]) \wedge (\text{VectorSpace}[V, +_v, *_v]) \wedge (\text{VectorSpace}[W, +_w, *_w]) \wedge \\ \left( \forall_{\alpha, \beta \in V} (L(\alpha +_v \beta) = L(\alpha) +_w L(\beta)) \right) \wedge \left( \forall_{r \in \mathbb{R}} \forall_{\alpha \in V} (L(r *_v \alpha) = r *_w L(\alpha)) \right) \end{array} \right)$$

$$\text{LinOp}[L, V, +_v, *_v] := \text{LinTrans}[L, V, +_v, *_v, V, +_v, *_v]$$

$$\mathcal{L}[V, W] := \{L \mid \text{LinTrans}[L, V, +_v, *_v, W, +_w, *_w]\}$$

$$\text{ZeroMapsToZero} := \forall_{L, V, W} \left( (\text{LinTrans}[L, V, +_v, *_v, W, +_w, *_w]) \implies (L(O_v) = O_w) \right)$$


---

(1)  $L(O_v) = L(O_v +_v O_v) = L(O_v) +_w L(O_v)$

---

(2)  $O_w = L(O_v) - L(O_v) = L(O_v)$

---

$$\text{SplitAddInv} := \forall_{L, V, W} \left( (\text{LinTrans}[L, V, +_v, *_v, W, +_w, *_w]) \implies \left( \forall_{\alpha, \beta \in V} (L(\alpha -_v \beta) = L(\alpha) -_w L(\beta)) \right) \right)$$


---

(1)  $L(\alpha - \beta) = L(\alpha + (-\beta)) = L(\alpha) + L(-\beta) = L(\alpha) + (-1) * L(\beta) = L(\alpha) - L(\beta)$

---

$$\text{UniqBasisLT} := \forall_{V, W} \left( \begin{array}{l} ((\text{VectorSpace}[V, +_v, *_v]) \wedge (\text{VectorSpace}[W, +_w, *_w]) \wedge (\text{Basis}[A, V, +_v, *_v]) \wedge (\text{Basis}[B, W, +_w, *_w])) \implies \\ \left( \exists!_T \left( (\text{LinTrans}[T, V, +_v, *_v, W, +_w, *_w]) \wedge \left( \forall_{i \in \mathbb{N}_{1,n}} (T(a_i) = b_i) \right) \right) \right) \end{array} \right)$$


---

(1)  $T(\sum_{i=1}^n (k_i * a_i)) := \sum_{i=1}^n (k_i * b_i)$

---

(2)  $(i \in \mathbb{N}_{1,n}) \implies \dots$

---

$$(2.1) \quad L := \left\langle \left\{ \begin{array}{cc} 1 & j = i \\ 0 & j \neq i \end{array} \right\} \mid j \in \mathbb{N}_{1,n} \right\rangle \quad \blacksquare \quad L \in \mathbb{R}^n$$


---

$$(2.2) \quad T(a_i) = T(\sum_{i=1}^n (l_i * a_i)) = \sum_{i=1}^n (l_i * b_i) = b_i \quad \blacksquare \quad T(a_i) = b_i$$


---

(3)  $(i \in \mathbb{N}_{1,n}) \implies (T(a_i) = b_i) \quad \blacksquare \quad \forall_{i \in \mathbb{N}_{1,n}} (T(a_i) = b_i)$

---

(4)  $(\text{BasisEquiv}) \wedge (\text{Basis}[A, V, +_v, *_v]) \quad \blacksquare \quad \forall_{v \in V} \exists!_{K \in \mathbb{R}^n} (\text{LinComb}[v, A, K, V, +, *]) \quad \dots$

---

(5)  $\dots \forall_{v_1, v_2 \in V} ((v_1 = v_2) \implies (T(v_1) = T(v_2))) \quad \blacksquare \quad \text{Function}[T, V, W]$

---

(6)  $(\alpha, \beta \in V) \implies \dots$

---

$$(6.1) \quad \left( \exists_{K_\alpha} (\text{LinComb}[\alpha, A, K_\alpha, V, +_v, *_v]) \right) \wedge \left( \exists_{K_\beta} (\text{LinComb}[\beta, A, K_\beta, V, +_v, *_v]) \right) \quad \blacksquare \quad (\alpha = \sum_{i=1}^n (k_{\alpha i} * a_i)) \wedge (\beta = \sum_{i=1}^n (k_{\beta i} * a_i))$$

$$(6.2) \quad T(\alpha + \beta) = T\left(\sum_{i=1}^n (k_{\alpha_i} * a_i) + \sum_{i=1}^n (k_{\beta_i} * a_i)\right) = T\left(\sum_{i=1}^n ((k_{\alpha_i} + k_{\beta_i}) * a_i)\right) = \sum_{i=1}^n ((k_{\alpha_i} + k_{\beta_i}) * b_i) = \dots$$

$$(6.3) \quad \dots \sum_{i=1}^n (k_{\alpha_i} * b_i) + \sum_{i=1}^n (k_{\beta_i} * b_i) = T\left(\sum_{i=1}^n (k_{\alpha_i} * a_i)\right) + T\left(\sum_{i=1}^n (k_{\beta_i} * a_i)\right) = T(\alpha) + T(\beta)$$

$$(7) \quad (\alpha, \beta \in V) \implies (L(\alpha +_v \beta) = L(\alpha) +_w L(\beta)) \quad \blacksquare \quad \forall_{\alpha, \beta \in V} (L(\alpha +_v \beta) = L(\alpha) +_w L(\beta))$$

$$(8) \quad ((r \in \mathbb{R}) \wedge (\alpha \in V)) \implies \dots$$

$$(8.1) \quad \exists_K (LinComb[\alpha, A, K, V, +_v, *_v]) \quad \blacksquare \quad \alpha = \sum_{i=1}^n (k_i * a_i)$$

$$(8.2) \quad L(r *_v \alpha) = L(r *_v \sum_{i=1}^n (k_i * a_i)) = L\left(\sum_{i=1}^n ((rk_i) *_v a_i)\right) = \dots$$

$$(8.3) \quad \dots \sum_{i=1}^n ((rk_i) *_w b_i) = r *_w \sum_{i=1}^n (k_i *_w b_i) = r *_w L\left(\sum_{i=1}^n (k_i *_v a_i)\right) = r *_w L(\alpha)$$

$$(9) \quad ((r \in \mathbb{R}) \wedge (\alpha \in V)) \implies (L(r *_v \alpha) = r *_w L(\alpha)) \quad \blacksquare \quad \forall_{r \in \mathbb{R}} \forall_{\alpha \in V} (L(r *_v \alpha) = r *_w L(\alpha))$$

$$(10) \quad \left(\forall_{i \in \mathbb{N}_{1,n}} (T(a_i) = b_i)\right) \wedge (Function[T, V, W]) \wedge \left(\forall_{\alpha, \beta \in V} (L(\alpha +_v \beta) = L(\alpha) +_w L(\beta))\right) \wedge \left(\forall_{r \in \mathbb{R}} \forall_{\alpha \in V} (L(r *_v \alpha) = r *_w L(\alpha))\right) \wedge \dots$$

$$(11) \quad \dots (VectorSpace[V, +_v, *_v]) \wedge (VectorSpace[W, +_w, *_w]) \quad \blacksquare \quad \left(\forall_{i \in \mathbb{N}_{1,n}} (T(a_i) = b_i)\right) \wedge (LinTrans[T, V, +_v, *_v, W, +_w, *_w])$$

$$(12) \quad \left(\left(\forall_{i \in \mathbb{N}_{1,n}} (T_2(a_i) = b_i)\right) \wedge (LinTrans[T_2, V, +_v, *_v, W, +_w, *_w])\right) \implies \dots$$

$$(12.1) \quad \forall_{i \in \mathbb{N}_{1,n}} (T_2(a_i) = b_i) \quad \blacksquare \quad \forall_{i \in \mathbb{N}_{1,n}} (T_2(c_i * a_i) = c_i * b_i) \quad \blacksquare \quad T_2\left(\sum_{i=1}^n (c_i * a_i)\right) = \sum_{i=1}^n (c_i * b_i) \quad \blacksquare \quad T_2 = T$$

$$(13) \quad \left(\left(\forall_{i \in \mathbb{N}_{1,n}} (T_2(a_i) = b_i)\right) \wedge (LinTrans[T_2, V, +_v, *_v, W, +_w, *_w])\right) \implies (T_2 = T)$$

$$+_L[S + T, S, T] := (S + T)(v) = S(v) + T(v)$$

$$*_L[r * T, r, T] := (r * T)(v) = r * (T(v))$$

$$LTVectorSpace := \forall_{V, W} (VectorSpace[\mathcal{L}[V, W], +_L, *_L])$$

(1) TODO

$$*_L[S * T, S, T] := (S * T)(v) = S(T(v))$$

$$LTProdProperties := (associativity) \wedge (identity) \wedge (distributive)$$

(1) TODO

$$Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w] := (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (ker_L = \{\alpha \in V \mid L(\alpha) = O_w\})$$

$$KerSubspace := \forall_{L, V, W} ((Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w]) \implies (Subspace[ker_L, V, +_v, *_v]))$$

$$(1) \quad ZeroMapsToZero \quad \blacksquare \quad L(O_v) = O_w \quad \blacksquare \quad O_v \in ker_L \quad \blacksquare \quad \emptyset \neq ker_L \quad \blacksquare \quad \emptyset \neq ker_L \subseteq V$$

$$(2) \quad (\alpha, \beta \in ker_L) \implies \dots$$

$$(2.1) \quad (L(\alpha) = O_w) \wedge (L(\beta) = O_w)$$

$$(2.2) \quad L(\alpha + \beta) = L(\alpha) + L(\beta) = O_w + O_w = O_w \quad \blacksquare \quad L(\alpha + \beta) \in ker_L$$

$$(3) \quad (\alpha, \beta \in ker_L) \implies (\alpha + \beta \in ker_L) \quad \blacksquare \quad \forall_{\alpha, \beta \in ker_L} (\alpha + \beta \in ker_L)$$

$$(4) \quad ((r \in \mathbb{R}) \wedge (\alpha \in ker_L)) \implies \dots$$

$$(4.1) \quad L(\alpha) = O_w \quad \blacksquare \quad L(r * \alpha) = r * L(\alpha) = r * O_w = O_w \quad \blacksquare \quad r * \alpha \in ker_L$$

$$(5) \quad ((r \in \mathbb{R}) \wedge (\alpha \in ker_L)) \implies (r * \alpha \in ker_L) \quad \blacksquare \quad \forall_{r \in \mathbb{R}} \forall_{\alpha \in ker_L} (r * \alpha \in ker_L)$$

$$(6) \quad (SubspaceEquiv) \wedge (\emptyset \neq ker_L \subseteq V) \wedge \left(\forall_{\alpha, \beta \in ker_L} (\alpha + \beta \in ker_L)\right) \wedge \left(\forall_{r \in \mathbb{R}} \forall_{\alpha \in ker_L} (r * \alpha \in ker_L)\right) \quad \blacksquare \quad Subspace[ker_L, V, +_v, *_v]$$

$$Rng[rng_L, L, V, +_v, *_v, W, +_w, *_w] := (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (rng_L = \{\beta \in W \mid \exists_{\alpha \in V} (\beta = L(\alpha))\})$$

$$RangeSubspace := \forall_{L, V, W} ((Ran[rng_L, L, V, +_v, *_v, W, +_w, *_w]) \implies (Subspace[rng_L, W, +_w, *_w]))$$

$$(1) \quad ZeroMapsToZero \quad \blacksquare \quad O_w = L(O_v) \quad \blacksquare \quad \exists_{\alpha \in V} (O_w = L(\alpha)) \quad \blacksquare \quad O_w \in rng_L \quad \blacksquare \quad \emptyset \neq rng_L \quad \blacksquare \quad \emptyset \neq rng_L \subseteq W$$

$$(2) \quad (\alpha, \beta \in rng_L) \implies \dots$$

$$\begin{aligned}
(2.1) \quad & \left( \exists_{u \in V} (\alpha = L(u)) \right) \wedge \left( \exists_{v \in V} (\beta = L(v)) \right) \\
(2.2) \quad & \alpha + \beta = L(u) + L(v) = L(u + v) \quad \blacksquare \quad \exists_{w \in V} (\alpha + \beta = L(w)) \quad \blacksquare \quad \alpha + \beta \in \text{rng}_L \\
(3) \quad & (\alpha, \beta \in \text{rng}_L) \implies (\alpha + \beta \in \text{rng}_L) \quad \blacksquare \quad \forall_{\alpha, \beta \in \text{rng}_L} (\alpha + \beta \in \text{rng}_L) \\
(4) \quad & ((r \in \mathbb{R}) \wedge (\alpha \in \text{rng}_L)) \implies \dots \\
(4.1) \quad & \exists_{v \in V} (\alpha = L(v)) \quad \blacksquare \quad L(r * v) = r * L(v) = r * \alpha \quad \blacksquare \quad \exists_{w \in V} (r * \alpha = L(w)) \quad \blacksquare \quad r * \alpha \in \text{rng}_L \\
(5) \quad & ((r \in \mathbb{R}) \wedge (\alpha \in \text{rng}_L)) \implies (r * \alpha \in \text{rng}_L) \quad \blacksquare \quad \forall_{r \in \mathbb{R}} \forall_{\alpha \in \text{rng}_L} (r * \alpha \in \text{rng}_L) \\
(6) \quad & (\text{SubspaceEquiv}) \wedge (\emptyset \neq \text{rng}_L \subseteq W) \wedge \left( \forall_{\alpha, \beta \in \text{rng}_L} (\alpha + \beta \in \text{rng}_L) \right) \wedge \left( \forall_{r \in \mathbb{R}} \forall_{\alpha \in \text{rng}_L} (r * \alpha \in \text{rng}_L) \right) \quad \blacksquare \quad \text{Subspace}[\text{rng}_L, W, +_w, *_w]
\end{aligned}$$

$$KerInj := \forall_{L, V, W} \left( (Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w]) \implies ((Inj[L, V, W]) \iff (ker_L = \{O_v\})) \right)$$

$$\begin{aligned}
(1) \quad & (Inj[L, V, W]) \implies \dots \\
(1.1) \quad & ZeroMapsToZero \quad \blacksquare \quad L(O_v) = O_w \\
(1.2) \quad & O_v \in ker_L \quad \blacksquare \quad \{O_v\} \subseteq ker_L \\
(1.3) \quad & (v \in ker_L) \implies \dots \\
(1.3.1) \quad & L(v) = O_w \\
(1.3.2) \quad & (Inj[L, V, W]) \wedge (L(O_v) = O_w) \quad \blacksquare \quad O_v = v \\
(1.4) \quad & (v \in ker_L) \implies (v = O_v) \quad \blacksquare \quad ker_L \subseteq \{O_v\} \\
(1.5) \quad & (\{O_v\} \subseteq ker_L) \wedge (ker_L \subseteq \{O_v\}) \quad \blacksquare \quad ker_L = \{O_v\} \\
(2) \quad & (Inj[L, V, W]) \implies (ker_L = \{O_v\}) \\
(3) \quad & (ker_L = \{O_v\}) \implies \dots \\
(3.1) \quad & \left( (u, v \in V) \wedge (L(u) = L(v)) \right) \implies \dots \\
(3.1.1) \quad & O_w = L(u) - L(v) = L(u - v) \quad \blacksquare \quad u - v \in ker_L \\
(3.1.2) \quad & ker_L = \{O_v\} \quad \blacksquare \quad u - v = O_v \quad \blacksquare \quad u = v \\
(3.2) \quad & \left( (u, v \in V) \wedge (L(u) = L(v)) \right) \implies (u = v) \quad \blacksquare \quad \forall_{u, v \in V} \left( (L(u) = L(v)) \implies (u = v) \right) \quad \blacksquare \quad Inj[L, V, W] \\
(4) \quad & (ker_L = \{O_v\}) \implies (Inj[L, V, W]) \\
(5) \quad & (Inj[L, V, W]) \iff (ker_L = \{O_v\})
\end{aligned}$$

$$RngSurj := \forall_{L, V, W} \left( (Ran[\text{rng}_L, L, V, +_v, *_v, W, +_w, *_w]) \implies ((Surj[L, V, W]) \iff (\text{rng}_L = W)) \right)$$

$$(1) \quad (SurjEquiv) \wedge (\text{rng}(L) = \text{rng}_L) \quad \blacksquare \quad (Surj[L, V, W]) \iff (\text{rng}_L = W)$$

$$RankNullityLT := \forall_{L, V, W} \left( (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \implies (Dim[V] = Dim[ker_L] + Dim[\text{rng}_L]) \right)$$

$$\begin{aligned}
(1) \quad & KerSubspace \quad \blacksquare \quad \left( \exists_U (Basis[U, ker_L, +_v, *_v]) \right) \wedge (Dim[ker_L] = |U|) \\
(2) \quad & (LinIndSuperspace) \wedge (LinInd[U, ker_L, +_v, *_v]) \quad \blacksquare \quad LinInd[U, V, +_v, *_v] \\
(3) \quad & (LinIndExpandBasis) \wedge (LinInd[U, V, +_v, *_v]) \quad \blacksquare \quad \left( \exists_B ((U \subseteq B) \wedge (Basis[B, V, +_v, *_v])) \right) \wedge (Dim[V] = |B|) \\
(4) \quad & U \subseteq B \quad \blacksquare \quad \exists_T (B = U \cup T) \\
(5) \quad & (w \in \text{rng}_L) \implies \dots \\
(5.1) \quad & \exists_{v \in V} (w = L(v)) \\
(5.2) \quad & (Basis[B, V, +_v, *_v]) \wedge (B = U \cup T) \quad \blacksquare \quad \exists_{K \in \mathbb{R}^{|B|}} \left( v = \sum_{i=1}^{|B|} (k_i * b_i) = \sum_{i=1}^{|U|} (k_i * u_i) + \sum_{i=1}^{|T|} (k_{|U|+i} * t_i) \right) \\
(5.3) \quad & w = L(v) = L \left( \sum_{i=1}^{|U|} (k_i * u_i) + \sum_{i=1}^{|T|} (k_{|U|+i} * t_i) \right) = L \left( \sum_{i=1}^{|U|} (k_i * u_i) \right) + L \left( \sum_{i=1}^{|T|} (k_{|U|+i} * t_i) \right) = \dots \\
(5.4) \quad & O + L \left( \sum_{i=1}^{|T|} (k_{|U|+i} * t_i) \right) = \sum_{i=1}^{|T|} (L(k_{|U|+i} * t_i)) = \sum_{i=1}^{|T|} (k_{|U|+i} * L(t_i)) \quad \blacksquare \quad \exists_K (LinComb[w, L(T), K, W, +, *]) \\
(6) \quad & (w \in \text{rng}_L) \implies \left( \exists_L (LinComb[w, L(T), L, W, +, *]) \right) \quad \blacksquare \quad Spans[L(T), \text{rng}_L, W, +, *] \\
(7) \quad & \left( (K \in \mathbb{R}^n) \wedge (LinComb[O_w, L(T), K, W, +_w, *_w]) \right) \implies \dots \\
(7.1) \quad & O_w = \sum_{i=1}^n (k_i * L(t_i)) = L \left( \sum_{i=1}^n (k_i * t_i) \right) \quad \blacksquare \quad \sum_{i=1}^n (k_i * t_i) \in ker_L
\end{aligned}$$



$$(7.3) \quad \text{Basis}[B] \quad \blacksquare \quad \text{LinInd}[B] \quad \blacksquare \quad \text{LinInd}[U \cup T] \quad \blacksquare \quad \forall_{s_j \in U \cup T} \forall_{K \in \mathbb{R}^{n-1}} (\neg \text{LinComb}[s_j, U \cup T \setminus \{s_j\}, K, V, +, *])$$

$$(7.4) \quad \left( \sum_{i=1}^n (k_i * t_i) = \sum_{i=1}^m (d_i * u_i) \right) \wedge \left( \forall_{s_j \in U \cup T} \forall_{K \in \mathbb{R}^{n-1}} (\neg LinComb[s_j, U \cup T \setminus \{s_j\}, K, V, +, *]) \right) \blacksquare (D = \{O\}) \wedge (K = \{O\})$$

$$(8) \quad \left( (K \in \mathbb{R}^n) \wedge (LinComb[O_w, L(T), K, W, +_w, *_w]) \right) \implies (K = \{O\}) \blacksquare LinInd[L(T), W, +_w, *_w]$$

(9)  $(SubIndependent) \wedge (LinInd[L(T), W, +_w, *_w]) \vdash LinInd[L(T), rng_L, +_w, *_w]$

$$(10) \quad (Spans[L(T), rng_L, W, +, *]) \wedge (LinInd[L(T), rng_L, +_w, *_w]) \blacksquare Basis[L(T), rng_L, +_w, *_w] \blacksquare Dim[rng_L] = |L(T)| = |T|$$

$$(11) \quad B = U \cup T \quad \blacksquare \quad |B| = |U| + |T| \quad \blacksquare \quad Dim[V] = Dim[ker_L] + Dim[rg_L]$$

$$InjSurjEqualDim := \forall_{T,V,W} \left( \begin{array}{l} ((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \wedge (Dim[V] = Dim[W]) \wedge (Inj[T, V, W])) \implies \\ (Surj[T, V, W]) \end{array} \right)$$

$$(1) \quad (KerInj) \wedge (Inj[T, V, W]) \quad \blacksquare \quad ker_T = \{O\} \quad \blacksquare \quad Dim[ker_T] = 0$$

$$(2) \quad (RankNullityLT) \wedge (Dim[ker_T] = 0) \quad \blacksquare \quad Dim[V] = Dim[ker_T] + Dim[rng_T] = Dim[rng_T] \quad \blacksquare \quad Dim[V] = Dim[rng_T]$$

$$(3) \quad (Dim[V] = Dim[W]) \wedge (Dim[V] = Dim[rng_T]) \quad \blacksquare \quad Dim[W] = Dim[rng_T]$$

(4) *RangeSubspace*  $\blacksquare$  *Subspace*[*rng<sub>T</sub>*, *W*,  $+_w$ ,  $*_w$ ]

$$(5) \quad (Subspace[rng_T, W, +_w, *_w]) \wedge (Dim[W] = Dim[rng_T]) \quad \blacksquare \quad \exists_B ((Basis[B, W, +_w, *_w]) \wedge (Basis[B, rng_T, +_w, *_w]))$$

$$(6) \quad (Spans[W] = Spans[rng_T]) \quad \blacksquare \quad W = rng_T \quad \blacksquare \quad Surj[T, V, W]$$

(1) *RankNullityLT* ■  $Dim[V] = Dim[ker_T] + Dim[rng_T]$

$$(2) \quad \text{Surj}[T, V, W] \quad \blacksquare \quad \text{rng}_T = W \quad \blacksquare \quad \text{Dim}[\text{rng}_T] = \text{Dim}[W]$$

(3)  $(Dim[V] = Dim[W]) \wedge (Dim[V] = Dim[ker_T] + Dim[rng_T]) \wedge (Dim[rng_T] = Dim[W]) \quad \blacksquare \quad Dim[ker_T] + Dim[rng_T] = Dim[rng_T]$   
 $\blacksquare \quad Dim[ker_T] = 0 \quad \blacksquare \quad ker_T = \{O\}$

---

(4)  $(KerInj) \wedge (er_T = \{O\}) \vdash Inj[T, V, W]$

$$(1) \quad (RankNullityLT) \wedge (Dim[W] \geq Dim[rng_T]) \quad \blacksquare \quad Dim[ker_T] = Dim[V] - Dim[rng_T] \geq Dim[V] - Dim[W] > 0 \quad \blacksquare \quad Dim[ker_T] \neq 0$$

$$(2) \quad (KerInj) \wedge (Dim[ker_T] \neq 0) \quad \vdash \quad \neg Inj[T, V, W]$$

(1) *RankNullityLT* ■  $\text{Dim}[\text{rng}_T] = \text{Dim}[V] - \text{Dim}[\text{ker}_T] \leq \text{Dim}[V] < \text{Dim}[W]$

$$(2) \quad \text{Dim}[\text{rng}_T] < \text{Dim}[W] \quad \vee \quad \text{Dim}[\text{rng}_T] \neq \text{Dim}[W] \quad \vee \quad \neg \text{Surj}[T, V, W]$$

A linear transformation  $L : V \rightarrow W$  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

$$(1) \quad L_1^{-1} = L_1^{-1} \circ 1_w = L_1^{-1} \circ (L \circ L_2^{-1}) = (L_1^{-1} \circ L) \circ L_2^{-1} = 1_v \circ L_2^{-1} = L_2^{-1} \quad \blacksquare \quad L_1^{-1} = L_2^{-1}$$

$$LTInvertible[L, V, +_v, *_v, W, +_w, *_w] := \exists_{L^{-1}}(LTInv[L^{-1}, L, V, +_v, *_v, W, +_w, *_w])$$

$$InvertibleBijEquiv := \forall_L \left( (LTInvertible[L, V, +_v, *_v, W, +_w, *_w]) \iff ((Inj[L, V, W]) \wedge (Surj[L, V, W])) \right)$$

$$(1) \quad (LTInvertible[L, V, +_v, *_v, W, +_w, *_w]) \implies \dots$$

$$(1.1) \quad \exists_{L^{-1}}(LTInv[L^{-1}, L, V, +_v, *_v, W, +_w, *_w])$$

$$(1.2) \quad (L(u) = L(w)) \implies \dots$$

$$(1.2.1) \quad u = L^{-1}(L(u)) = L^{-1}(L(w)) = w \quad \blacksquare \quad u = w$$

$$(1.3) \quad (L(u) = L(w)) \implies (u = w) \quad \blacksquare \quad \forall_{u,w} \left( (L(u) = L(w)) \implies (u = w) \right) \quad \blacksquare \quad Inj[L, V, W]$$

$$(1.4) \quad (w \in W) \implies \dots$$

$$(1.4.1) \quad L^{-1}(w) \in V$$

$$(1.4.2) \quad L \circ L^{-1} = 1_w \quad \blacksquare \quad L(L^{-1}(w) = w)$$

$$(1.4.3) \quad (L^{-1}(w) \in V) \wedge (L(L^{-1}(w)) = w) \quad \blacksquare \quad \exists_{v \in V} (w = L(v))$$

$$(1.5) \quad (w \in W) \implies \left( \exists_{v \in V} (w = L(v)) \right) \quad \blacksquare \quad \forall_{w \in W} \exists_{v \in V} (w = L(v)) \quad \blacksquare \quad Surj[L, V, W]$$

$$(1.6) \quad (Inj[L, V, W]) \wedge (Surj[L, V, W])$$

$$(2) \quad (LTInvertible[L, V, +_v, *_v, W, +_w, *_w]) \implies ((Inj[L, V, W]) \wedge (Surj[L, V, W]))$$

$$(3) \quad ((Inj[L, V, W]) \wedge (Surj[L, V, W])) \implies \dots$$

$$(3.1) \quad (Inj[L, V, W]) \wedge (Surj[L, V, W]) \quad \blacksquare \quad \forall_{w \in W} \exists!_{v \in V} (w = L(v))$$

$$(3.2) \quad S := \{(w, v) \in W \times V \mid w = L(v)\}$$

$$(3.3) \quad \left( \forall_{w \in W} \exists!_{v \in V} (w = L(v)) \right) \wedge (S = \{(w, v) \in W \times V \mid w = L(v)\}) \quad \blacksquare \quad Function[S, W, V]$$

$$(3.4) \quad \left( \forall_{v \in V} (S(L(v)) = v) \right) \wedge \left( \forall_{w \in W} (L(S(w)) = w) \right)$$

$$(3.5) \quad (w_1, w_2 \implies W) \implies \dots$$

$$(3.5.1) \quad (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge \left( \forall_{w \in W} (L(S(w)) = w) \right) \quad \blacksquare \quad L(S(w_1) + S(w_2)) = L(S(w_1)) + L(S(w_2)) = w_1 + w_2$$

$$(3.5.2) \quad \left( \forall_{w \in W} (L(S(w)) = w) \right) \wedge (w_1 + w_2 \in W) \quad \blacksquare \quad L(S(w_1 + w_2)) = w_1 + w_2$$

$$(3.5.3) \quad L(S(w_1) + S(w_2)) = w_1 + w_2 = L(S(w_1 + w_2)) \quad \blacksquare \quad L(S(w_1) + S(w_2)) = L(S(w_1 + w_2))$$

$$(3.5.4) \quad (Inj[L, V, W]) \wedge (L(S(w_1) + S(w_2)) = L(S(w_1 + w_2))) \quad \blacksquare \quad S(w_1) + S(w_2) = S(w_1 + w_2)$$

$$(3.6) \quad (w_1, w_2 \implies W) \implies (S(w_1 + w_2) = S(w_1) + S(w_2)) \quad \blacksquare \quad \forall_{w_1, w_2 \in W} (S(w_1 + w_2) = S(w_1) + S(w_2))$$

$$(3.7) \quad (r \in \mathbb{R}) \wedge (w \in W) \implies \dots$$

$$(3.7.1) \quad (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge \left( \forall_{w \in W} (L(S(w)) = w) \right) \quad \blacksquare \quad L(r * S(w)) = r * L(S(w)) = r * w$$

$$(3.7.2) \quad \left( \forall_{w \in W} (L(S(w)) = w) \right) \wedge (r * w \in W) \quad \blacksquare \quad L(S(r * w)) = r * w$$

$$(3.7.3) \quad L(r * S(w)) = r * w = L(S(r * w)) \quad \blacksquare \quad L(r * S(w)) = L(S(r * w))$$

$$(3.7.4) \quad (Inj[L, V, W]) \wedge (L(r * S(w)) = L(S(r * w))) \quad \blacksquare \quad r * S(w) = S(r * w)$$

$$(3.8) \quad (r \in \mathbb{R}) \wedge (w \in W) \implies (r * S(w) = S(r * w)) \quad \blacksquare \quad \forall_{r \in \mathbb{R}} \forall_{w \in W} (S(r * w) = r * S(w))$$

$$(3.9) \quad (Function[S, W, V]) \wedge \left( \forall_{w_1, w_2 \in W} (S(w_1 + w_2) = S(w_1) + S(w_2)) \right) \wedge \left( \forall_{r \in \mathbb{R}} \forall_{w \in W} (S(r * w) = r * S(w)) \right)$$

$$(3.10) \quad LinTrans[S, W, +_w, *_w, V, +_v, *_v]$$

$$(3.11) \quad \forall_{v \in V} \left( (S(L(v)) = v) \right) \quad \blacksquare \quad S \circ L = 1_v$$

$$(3.12) \quad \forall_{w \in W} \left( L(S(w)) = w \right) \blacksquare L \circ S = 1_w$$

$$(3.13) \quad (LinTrans[S, W, +_w, *_w, V, +_v, *_v]) \wedge (S \circ L = 1_v) \wedge (L \circ S = 1_w) \blacksquare LTInv[S, L, V, +_v, *_v, W, +_w, *_w]$$

$$(3.14) \quad \exists_{L^{-1}}(LTInv[L^{-1}, L, V, +_v, *_v, W, +_w, *_w]) \blacksquare LTInvertible[L, V, +_v, *_v, W, +_w, *_w]$$

$$(4) \quad ((Inj[L, V, W]) \wedge (Surj[L, V, W])) \implies (LTInvertible[L, V, +_v, *_v, W, +_w, *_w])$$

$$(5) \quad (LTInvertible[L, V, +_v, *_v, W, +_w, *_w]) \iff ((Inj[L, V, W]) \wedge (Surj[L, V, W]))$$

TODO: some corollary of InjSurjEqualDim + SurjInjEqualDim + InvertibleBijEquiv

$$Isomorphism[L, V, +_v, *_v, W, +_w, *_w] := LTInvertible[L, V, +_v, *_v, W, +_w, *_w]$$

$$Isomorphic[V, +_v, *_v, W, +_w, *_w] := \exists_L(Isomorphism[L, V, +_v, *_v, W, +_w, *_w])$$

### 3.9 Matrix of a Linear Transform

$$CoordVec[[\alpha]_S, \alpha, S, V, +, *] := (Basis[S, V, +, *]) \wedge (S * [\alpha]_S = \alpha \in V)$$

$$LTMatrix := \forall_{L, V, W} \left( \begin{array}{l} ((LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (Basis[A, V, +_v, *_v]) \wedge (Basis[B, W, +_w, *_w])) \implies \\ \left( \forall_{v \in V} (CoordVec[[L(v)]_B, L(v), B, W, +_w, *_w] = \langle [L(a_i)]_B \mid a_i \in A \rangle * CoordVec[[v]_A, v, A, V, +_v, *_v]) \right) \end{array} \right)$$

$$(1) \quad Basis[A, V, +_v, *_v] \blacksquare \exists_{K \in \mathbb{R}^n} (v = \sum_{i=1}^n (k_i * a_i)) \blacksquare K^T = CoordVec[[v]_A, v, A, V, +, *]$$

$$(2) \quad [L(v)]_B = [L(\sum_{i=1}^n (k_i * a_i))]_B = [\sum_{i=1}^n (L(k_i * a_i))]_B = \sum_{i=1}^n ([L(k_i * a_i)]_B) = \sum_{i=1}^n ([k_i * L(a_i)]_B) = \sum_{i=1}^n (k_i * [L(a_i)]_B) = \dots$$

$$(3) \quad \dots \langle [L(a)]_B \mid a \in A \rangle * K^T = \langle [L(a)]_B \mid a \in A \rangle * [v]_A \blacksquare [L(v)]_B = \langle [L(a)]_B \mid a \in A \rangle * [v]_A$$

Note: Shorthand is to RREF the augmented matrix [Columns of B | Columns of A] into [I | M], thus M is the transition matrix

$$TransitionMatrix := \forall_{L, V} \left( \begin{array}{l} ((Basis[A, V, +, *]) \wedge (Basis[B, V, +, *])) \implies \\ \left( \forall_{v \in V} (CoordVec[[v]_B, v, B, W, +_w, *_w] = \langle [a]_B \mid a \in A \rangle * CoordVec[[v]_A, v, A, V, +_v, *_v]) \right) \end{array} \right)$$

$$(1) \quad (LTMatrix) \wedge (LinTrans[I, V, +, *, V, +, *]) \blacksquare [I(v)]_B = \langle [I(a)]_B \mid a \in A \rangle * [v]_A \blacksquare [v]_B = \langle [a]_B \mid a \in A \rangle * [v]_A$$

$$LTOverTransition := \left( ([L(a)]_T = A * [a]_S) \wedge (P * [a]_{S'} = [a]_S) \wedge (Q * [L(a)]_{T'} = [L(a)]_T) \right) \implies ([L(a)]_{T'} = (Q^{-1} * A * P) * [a]_{S'})$$

$$(1) \quad [L(a)]_{T'} = Q^{-1} * [L(a)]_T = Q^{-1} * A * [a]_S = Q^{-1} * A * P * [a]_{S'} \blacksquare [L(a)]_{T'} = (Q^{-1} * A * P) * [a]_{S'}$$

$$LOOverTransition := \left( ([L(a)]_S = A * [a]_S) \wedge (P * [a]_{S'} = [a]_S) \right) \implies ([L(a)]_{S'} = (P^{-1} * A * P) * [a]_{S'})$$

$$(1) \quad P * [a]_{S'} = [a]_S \blacksquare P * [L(a)]_{S'} = [L(a)]_S$$

$$(2) \quad LTOverTransition \blacksquare [L(a)]_{S'} = P^{-1} * [L(a)]_S = P^{-1} * A * [a]_S = P^{-1} * A * P * [a]_{S'} \blacksquare [L(a)]_{S'} = (P^{-1} * A * P) * [a]_{S'}$$

$$RankNullityRelation := (Rank[A] \equiv Dim[rng_L]) \wedge (Nullity[A] \equiv Dim[ker_L]) \wedge (RankNullity \equiv RankNullityLT)$$

$$(1) \quad \text{TODO}$$

$$SimMatrix[A, B] := \exists_P (B = P * A * P^{-1})$$

$$SimMatrixEquiv := (SimMatrix[A, B]) \iff \left( \exists_{S, T, S', T'} \left( ([L(a)]_T = A * [a]_S) \wedge ([L(a)]_{T'} = B * [a]_{S'}) \right) \right)$$

$$(1) \quad \text{TODO}$$

$$SimRank := (SimMatrix[A, B]) \implies (Rank[A] = Rank[B])$$

$$(1) \quad \text{TODO}$$

### 3.10 Determinants

$$Perm[\sigma, S] := Bij[\sigma, S, S]$$

$$IntPermSet[S_n, n] := S_n = \{\sigma \mid Perm[\sigma, \mathbb{N}_{1,n}]\}$$

$$IntPermSetCard := (IntPermSet[S_n, n]) \implies (|S_n| = n!)$$

$$(1) \quad |S_1| = |\{(1)\}| = 1 = 1!$$

$$(2) \quad (|S_m| = m!) \implies \dots$$

$$(2.1) \quad |S_{m+1}| = |\mathbb{N}_{1,m+1} \times S_m| = (m+1)(m!) = (m+1)!$$

$$(3) \quad (|S_m| = m!) \implies (|S_{m+1}| = (m+1)!)$$

$$(4) \quad S_n = \{\sigma \mid Perm[\sigma, \mathbb{N}_{1,n}]\}$$

$$IntPermGroup := Group[S_n, \circ]$$

$$(1) \quad Perm[I_n, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \blacksquare I_n \in S_n$$

$$(2) \quad (\sigma, \tau, v \in S_n) \implies \dots$$

$$(2.1) \quad (Bij[\sigma, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \wedge (Bij[\tau, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \blacksquare Bij[\sigma \circ \tau, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \blacksquare \sigma \circ \tau \in S_n)$$

$$(2.2) \quad (Bij[\sigma, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \wedge (Bij[\tau, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \wedge (Bij[v, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \blacksquare (\sigma \circ \tau) \circ v = \sigma \circ (\tau \circ v))$$

$$(2.3) \quad \sigma \circ I_n = \sigma = I_n \circ \sigma$$

$$(2.4) \quad Bij[\sigma, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \blacksquare \sigma \circ \sigma^{-1} = I_n = \sigma^{-1} \circ \sigma$$

$$(3) \quad Group[S_n, \circ]$$

$$IntPermSetEquiv := (IntPermSet[S_n, n]) \wedge (\tau \in S_n) \implies (S_n = \{\tau \circ \sigma \mid \sigma \in S_n\} = \{\sigma \circ \tau \mid \sigma \in S_n\} = \{\sigma^{-1} \mid \sigma \in S_n\})$$

$$(1) \quad (\alpha \in S_n) \iff (\alpha = \tau \circ (\tau^{-1} \circ \alpha) \in S_n) \iff (\alpha \in \{\tau \circ \sigma \mid \sigma \in S_n\})$$

$$(2) \quad (\alpha \in S_n) \iff (\alpha = (\alpha \circ \tau^{-1}) \circ \tau \in S_n) \iff (\alpha \in \{\sigma \circ \tau \mid \sigma \in S_n\})$$

$$(3) \quad (\alpha \in S_n) \iff (\alpha = (\alpha^{-1})^{-1} \in S_n) \iff (\alpha \in \{\sigma^{-1} \mid \sigma \in S_n\})$$

$$(4) \quad S_n = \{\tau \circ \sigma \mid \sigma \in S_n\} = \{\sigma \circ \tau \mid \sigma \in S_n\} = \{\sigma^{-1} \mid \sigma \in S_n\}$$

$$Inversions[n(\sigma), \sigma] := (\sigma \in S_n) \wedge \left( n(\sigma) = |\{(i, j) \mid (i < j) \wedge (\sigma(i) > \sigma(j))\}| = \sum_{i=1}^n \left( |\{(i, j) \mid (\sigma(i) > \sigma(j)) \wedge (i < j \leq n)\}| \right) \right)$$

$$Transposition[\tau, m, r] := (\tau \in S_n) \wedge \left( \forall_{i \in \mathbb{N}_{1,n}} \left( (i \notin \{m, r\}) \implies (\tau(i) = i) \right) \right) \wedge (\tau(m) = r) \wedge (\tau(r) = m)$$

$$TranspositionInv := (Transposition[\tau]) \implies (\tau = \tau^{-1})$$

$$(1) \quad \tau \circ \tau^{-1} = I_n \blacksquare \tau = \tau^{-1}$$

$$TranspositionDecomp := (\sigma \in S_n) \implies \left( \exists_T \left( (Transpositions[T]) \wedge \left( \sigma = \circ_{\tau_i \in T} (\tau_i) \right) \right) \right)$$

$$(1) \quad (n(\sigma) = 0) \implies \dots$$

$$(1.1) \quad \sigma = I_n$$

$$(1.2) \quad (Transpositions[\{(12), (12)\}]) \wedge (\sigma = I_n = (12) \circ (12))$$

$$(1.3) \quad \exists_T \left( (Transpositions[T]) \wedge \left( \sigma = \circ_{\tau_i \in T} (\tau_i) \right) \right)$$

$$(2) \quad (n(\sigma) = 0) \implies \left( \exists_T \left( (Transpositions[T]) \wedge \left( \sigma = \circ_{\tau_i \in T} (\tau_i) \right) \right) \right)$$

$$(3) \quad \left( n(\sigma) = k+1 \right) \wedge \left( \forall_{\sigma' \in S_n} \left( n(\sigma') \leq k \implies \left( \exists_T \left( (Transpositions[T]) \wedge \left( \sigma' = \circ_{\tau_i \in T} (\tau_i) \right) \right) \right) \right) \right) \implies \dots$$

$$(3.1) \quad n(\sigma) = k+1 \blacksquare n(\sigma) > 1 \blacksquare \exists_{l \in \mathbb{N}} \left( (\sigma(l) \neq l) \wedge \left( \forall_{i \in \mathbb{N}_{1,l}} (\sigma(i) = i) \right) \right)$$

---


$$(3.2) \quad \text{Transposition}[\delta, l, \tau(l)] \quad \blacksquare \quad n(\delta \circ \sigma) < n(\sigma)$$


---

$$(3.3) \quad \forall_{\sigma' \in S_n} \left( n(\sigma') \leq k \right) \implies \left( \exists_T \left( (\text{Transpositions}[T]) \wedge \left( \sigma' = \circ_{\tau_i \in T}(\tau_i) \right) \right) \right) \blacksquare \exists_{T'} \left( (\text{Transpositions}[T']) \wedge \left( \delta \circ \sigma = \circ_{\tau_i \in T'}(\tau_i) \right) \right)$$


---

$$(3.4) \quad \sigma = \delta^{-1} \circ \circ_{\tau_i \in T'}(\tau_i) = \delta \circ \circ_{\tau_i \in T'}(\tau_i) = \circ_{\tau_i \in T''}(\tau_i)$$


---

$$(3.5) \quad \exists_{T''} \left( (\text{Transpositions}[T'']) \wedge \left( \sigma = \circ_{\tau_i \in T''}(\tau_i) \right) \right)$$


---

$$(4) \quad \left( n(\sigma) = k + 1 \right) \wedge \left( \forall_{\sigma' \in S_n} \left( n(\sigma') \leq k \implies \left( \exists_T \left( (\text{Transpositions}[T]) \wedge \left( \sigma' = \circ_{\tau_i \in T}(\tau_i) \right) \right) \right) \right) \right) \implies \dots$$


---

$$(5) \quad \dots \left( \exists_{T''} \left( (\text{Transpositions}[T'']) \wedge \left( \sigma = \circ_{\tau_i \in T''}(\tau_i) \right) \right) \right)$$


---

$$(6) \quad \text{Induction} \quad \blacksquare \quad \exists_T \left( (\text{Transpositions}[T]) \wedge \left( \sigma = \circ_{\tau_i \in T}(\tau_i) \right) \right)$$


---