

# Contents

<b>1</b>	<b>Real Analysis</b>	<b>3</b>
<b>2</b>	<b>Abstract Algebra</b>	<b>15</b>
2.1	Functions	15
2.2	Divisibility, Equivalence Relations, Partitions	15
2.3	Groups	16
2.4	Subgroups	17
2.5	Special Groups	18
2.5.1	Cyclic Group	18
2.5.2	Symmetric and Alternating Groups	19
2.5.3	Dihedral Group	19
2.6	Lagrange's Theorem	19
2.7	Homomorphisms	20
2.8	Kernel and Image Homomorphisms	21
2.9	Conjugacy	23
2.10	Normal Subgroups	24
2.11	Quotient Groups	25
<b>3</b>	<b>Linear Algebra</b>	<b>29</b>
3.1	Matrix Operations and Special Matrices	29
3.2	Elementary Matrices on Invertibility and Systems of Linear Equations	31
3.3	Vector Spaces	33
3.4	Subspaces and Special Subspaces	34
3.5	Linear Combination, Linear Span, Linear Independence	36
3.6	Bases and Dimensions	39
3.7	Rank	40
3.8	Linear Transformations	41
3.9	Matrix of a Linear Transform	45
3.10	Determinants	46



# Chapter 1

## Real Analysis

(1.5)

*OrderTrichotomy* $[\prec, S] := \forall_{x,y \in S} (x \prec y \vee x = y \vee y \prec x)$

*OrderTransitivity* $[\prec, S] := \forall_{x,y,z \in S} ((x \prec y \wedge y \prec z) \implies x \prec z)$

*Order* $[\prec, S] := (\textcolor{teal}{OrderTrichotomy}[\prec, S]) \wedge (\textcolor{teal}{OrderTransitivity}[\prec, S])$

(1.7)

*Bounded Above* $[E, S, \prec] := (\textcolor{teal}{Order}[\prec, S]) \wedge (E \subset S) \wedge (\exists_{\beta \in S} \forall_{x \in E} (x \leq \beta))$

*Bounded Below* $[E, S, \prec] := (\textcolor{teal}{Order}[\prec, S]) \wedge (E \subset S) \wedge (\exists_{\beta \in S} \forall_{x \in E} (\beta \leq x))$

*Upper Bound* $[\beta, E, S, \prec] := (\textcolor{teal}{Order}[\prec, S]) \wedge (E \subset S) \wedge (\beta \in S \wedge \forall_{x \in E} (x \leq \beta))$

*Lower Bound* $[\beta, E, S, \prec] := (\textcolor{teal}{Order}[\prec, S]) \wedge (E \subset S) \wedge (\beta \in S \wedge \forall_{x \in E} (\beta \leq x))$

(1.8)

*LU B* $[\alpha, E, S, \prec] := (\textcolor{teal}{Upper Bound}[\alpha, E, S, \prec]) \wedge (\forall_{\gamma} (\gamma < \alpha \implies \neg \textcolor{teal}{Upper Bound}[\gamma, E, S, \prec]))$

*GLB* $[\alpha, E, S, \prec] := (\textcolor{teal}{Lower Bound}[\alpha, E, S, \prec]) \wedge (\forall_{\beta} (\alpha < \beta \implies \neg \textcolor{teal}{Lower Bound}[\beta, E, S, \prec]))$

(1.10)

*LU B Property* $[S, \prec] := \forall_E (((\emptyset \neq E \subset S) \wedge (\textcolor{teal}{Bounded Above}[E, S, \prec]) \implies \exists_{\alpha \in S} (\textcolor{teal}{LU B}[\alpha, E, S, \prec])))$

*GLB Property* $[S, \prec] := \forall_E (((\emptyset \neq E \subset S) \wedge (\textcolor{teal}{Bounded Below}[E, S, \prec]) \implies \exists_{\alpha \in S} (\textcolor{teal}{GLB}[\alpha, E, S, \prec])))$

(1.11)

*LU B Property Implies GLB Property*  $:= \textcolor{teal}{LU B Property}[S, \prec] \implies \textcolor{teal}{GLB Property}[S, \prec]$

(1)  $\textcolor{teal}{LU B Property}[S, \prec] \implies \dots$

wts: 2

(1.1)  $(\emptyset \neq B \subset S \wedge \textcolor{teal}{Bounded Below}[B, S, \prec]) \implies \dots$

wts: 1.2

from: *Bounded Below*, 1.1

(1.1.1)  $\textcolor{teal}{Order}[\prec, S] \wedge \exists_{\delta' \in S} (\textcolor{teal}{Lower Bound}[\delta', B, S, \prec])$

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

wts: 1.1.3

from: 1.1.2

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

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

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

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

wts: 1.1.5

from: *LU B Property*, 1

(1.1.4.1)  $\forall_E (((\emptyset \neq E \subset S \wedge \textcolor{teal}{Bounded Above}[E, S, \prec]) \implies \exists_{\alpha \in S} (\textcolor{teal}{LU B}[\alpha, E, S, \prec])))$

(1.1.4.2)  $L := \{s \in S : \textcolor{teal}{Lower Bound}[s, B, S, \prec]\}$

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

from: *Order*, 1.1.1  
wts: 1.1.4.7

(1.1.4.4)  $b_1 := \textit{choice}(\{b_1' \in B : \exists_{b_0' \in B} (b_0' < b_1')\}) \blacksquare \neg \textcolor{teal}{Lower Bound}[b_1, B, S, \prec]$

from: 1.1.4.2

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

(1.1.4.6)  $\delta := \textit{choice}(\{\delta' \in S : \textcolor{teal}{Lower Bound}[\delta', B, S, \prec]\}) \blacksquare \delta \in L \blacksquare \emptyset \neq L$

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)  $\forall_{y \in L} (\textcolor{teal}{Lower Bound}[y_0, B, S, \prec]) \blacksquare \forall_{y \in L} \forall_{x \in B} (y_0 \leq x)$

from: *Lower Bound*, 1.1.4.2  
wts: 1.1.4.10

(1.1.4.9)  $\forall_{x \in B} (x \in S \wedge \forall_{y \in L} (y_0 \leq x)) \blacksquare \forall_{x \in B} (\textcolor{teal}{Upper Bound}[x, L, S, \prec])$

from: *Upper Bound*

(1.1.4.10)  $\exists_{x \in S} (\textcolor{teal}{Upper Bound}[x, L, S, \prec]) \blacksquare \textcolor{teal}{Bounded Above}[L, S, \prec]$

(1.1.4.11)	$\emptyset \neq L \subset S \wedge \text{Bounded Above}[L, S, <]$	from: 1.1.4.7, 1.1.4.10
(1.1.4.12)	$\exists_{\alpha' \in S}(\text{LUB}[\alpha', L, S, <]) \blacksquare \alpha := \text{choice}(\{\alpha' \in S : (\text{LUB}[\alpha', L, S, <])\})$	from: 1.1.4.1 wts: 1.1.4.21
(1.1.4.13)	$\forall_x(x \in B \implies \text{Upper Bound}[x, L, S, <])$	from: 1.1.4.9 wts: 1.1.4.17
(1.1.4.14)	$\forall_x(\neg \text{Upper Bound}[x, L, S, <] \implies x \notin B)$	
(1.1.4.15)	$\gamma < \alpha \implies \dots$	wts: 1.1.4.16
(1.1.4.15.1)	$\neg \text{Upper Bound}[\gamma, L, S, <] \blacksquare \gamma \notin B$	from: LUB, 1.1.4.12, 1.1.4.14
(1.1.4.16)	$\gamma < \alpha \implies \gamma \notin B \blacksquare \gamma \in B \implies \gamma \geq \alpha$	
(1.1.4.17)	$\forall_{\gamma \in B}(\alpha \leq \gamma) \blacksquare \text{Lower Bound}[\alpha, B, S, <]$	from: Lower Bound
(1.1.4.18)	$\alpha < \beta \implies \dots$	wts: 1.1.4.19
(1.1.4.18.1)	$\forall_{y \in L}(y_0 \leq \alpha < \beta) \blacksquare \forall_{y \in L}(y_0 \neq \beta)$	from: LUB, 1.1.4.12, 1.1.4.18
(1.1.4.18.2)	$\beta \notin L \blacksquare \neg \text{Lower Bound}[\beta, B, S, <]$	from: 1.1.4.2
(1.1.4.19)	$\alpha < \beta \implies \neg \text{Lower Bound}[\beta, B, S, <] \blacksquare \forall_{\beta \in S}(\alpha < \beta \implies \neg \text{Lower Bound}[\beta, B, S, <])$	
(1.1.4.20)	$\text{Lower Bound}[\alpha, B, S, <] \wedge \forall_{\beta \in S}(\alpha < \beta \implies \neg \text{Lower Bound}[\beta, B, S, <])$	from: 1.1.4.17, 1.1.4.19
(1.1.4.21)	$\text{GLB}[\alpha, B, S, <] \blacksquare \exists_{\epsilon_1 \in S}(\text{GLB}[\epsilon_1, B, S, <])$	
(1.1.5)	$ B  \neq 1 \implies \exists_{\epsilon_1 \in S}(\text{GLB}[\epsilon_1, B, S, <])$	
(1.1.6)	$( B  = 1 \implies \exists_{\epsilon_0 \in S}(\text{GLB}[\epsilon_0, B, S, <])) \wedge ( B  \neq 1 \implies \exists_{\epsilon_1 \in S}(\text{GLB}[\epsilon_1, B, S, <]))$	from: 1.1.3, 1.1.5
(1.1.7)	$( B  = 1 \vee  B  \neq 1) \implies \exists_{\epsilon \in S}(\text{GLB}[\epsilon, B, S, <]) \blacksquare \exists_{\epsilon \in S}(\text{GLB}[\epsilon, B, S, <])$	
(1.2)	$(\emptyset \neq B \subset S \wedge \text{Bounded Below}[B, S, <]) \implies \exists_{\epsilon \in S}(\text{GLB}[\epsilon, B, S, <])$	
(1.3)	$\forall_B((\emptyset \neq B \subset S \wedge \text{Bounded Below}[B, S, <]) \implies \exists_{\epsilon \in S}(\text{GLB}[\epsilon, B, S, <]))$	
(1.4)	$\text{GLBProperty}[S, <]$	
(2)	$\text{LUBProperty}[S, <] \implies \text{GLBProperty}[S, <]$	

(1.12)

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

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

(1.14)

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

(1)	$y = 0 + y = (x + (-x)) + y = ((-x) + x) + y = (-x) + (x + y) = \dots$	from: Field
-----	--	-------------

(2)	$(-x) + (x + z) = ((-x) + x) + z = (x + (-x)) + z = 0 + z = z$	from: Field
-----	--	-------------

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

(1)	$x + y = x = 0 + x = x + 0$	from: Field
-----	-----------------------------	-------------

(2)	$y = 0$	from: AdditiveCancellation
-----	---------	----------------------------

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

(1)	$x + y = 0 = x + (-x)$	from: Field
-----	------------------------	-------------

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

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

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

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

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

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

from: [Field](#)

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

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)

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

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

(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

$$(1.19)$$

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

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

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

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

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

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

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

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

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

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

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

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

$$(1.4) \quad q \notin \alpha \implies p < q \quad \blacksquare \quad p < q$$

from: 1

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

---

**CutCorollaryI1**  $:= (\alpha \in \mathbb{R} \wedge r, s \in \mathbb{Q} \wedge r < s \wedge r \notin \alpha) \implies s \notin \alpha$

---

(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: [CutI1](#), 1

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

---

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

**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: [CutCorollaryI](#)

(1.1.3.3)  $q \in \alpha$

---

from: [CutI1](#)

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

---

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

---

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

---

from: [OrderTrichotomyR](#), [OrderTransitivityR](#)  
wts:

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

---

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

---

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

---

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

---

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

---

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

---

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

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

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

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

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

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

(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)	$\exists_a(a \in \alpha) ; \exists_b(b \in \beta) \blacksquare a_0 := \text{choice}(\{a : a \in \alpha\}) ; b_0 := \text{choice}(\{b : b \in \beta\}) \blacksquare a_0 + b_0 \in \alpha +_{\mathbb{R}} \beta$
(1.4)	$\exists_x(x \notin \alpha) ; \exists_y(y_0 \notin \beta) \blacksquare x_0 := \text{choice}(\{x : x \notin \alpha\}) ; y_0 := \text{choice}(\{y : y \notin \beta\})$
(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)	$\emptyset \neq \alpha +_{\mathbb{R}} \beta \subset \mathbb{Q} \blacksquare \text{CutI}[\alpha +_{\mathbb{R}} \beta]$



- (1.7)  $(p \in \alpha +_{\mathbb{R}} \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies \dots$
- (1.7.1)  $\exists_{r \in \alpha} \exists_{s \in \beta} (p = r + s) \blacksquare (r_0, s_0) := \text{choice}((r, s) \in \alpha \times \beta : p = r + s)$
- (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)  $(p \in \alpha +_{\mathbb{R}} \beta \wedge q \in \mathbb{Q} \wedge q < p) \implies q \in \alpha +_{\mathbb{R}} \beta \blacksquare \forall_{p \in \alpha +_{\mathbb{R}} \beta} \forall_{q \in \mathbb{Q}} (q < p \implies q \in \alpha +_{\mathbb{R}} \beta) \blacksquare \text{CutII}[\alpha +_{\mathbb{R}} \beta]$
- (1.9)  $p \in \alpha \implies \dots$
- (1.9.1)  $\exists_{r \in \alpha} \exists_{s \in \beta} (p = r + s) \blacksquare (r_1, s_1) := \text{choice}(\{(r, s) \in \alpha \times \beta : p = r + s\})$
- (1.9.2)  $r_1 \in \alpha \blacksquare \exists_{t \in \alpha} (r_1 < t) \blacksquare t_0 := \text{choice}(\{t \in \alpha : r_1 < t\})$
- (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)  $p \in \alpha \implies \exists_{r \in \alpha +_{\mathbb{R}} \beta} (p < r) \blacksquare \forall_{p \in \alpha +_{\mathbb{R}} \beta} \exists_{r \in \alpha +_{\mathbb{R}} \beta} (p < r) \blacksquare \text{CutIII}[\alpha +_{\mathbb{R}} \beta]$
- (1.11)  $\text{CutI}[\alpha +_{\mathbb{R}} \beta] \wedge \text{CutII}[\alpha +_{\mathbb{R}} \beta] \wedge \text{CutIII}[\alpha +_{\mathbb{R}} \beta] \blacksquare \alpha +_{\mathbb{R}} \beta \in \mathbb{R}$
- (2)  $(\alpha, \beta \in \mathbb{R}) \implies ((\alpha +_{\mathbb{R}} \beta) \in \mathbb{R})$

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

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

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

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

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

- (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)  $\exists_{r \in \alpha} (p < r) \blacksquare r_2 := \text{choice}(\{r \in \alpha : p < r\})$
- (1.4.2)  $p < r_2 \blacksquare p - r_2 < r_2 - r_2 = 0 \blacksquare (p - r_2) < 0 \blacksquare (p - r_2) \in 0_{\mathbb{R}}$
- (1.4.3)  $r_2 \in \alpha \blacksquare p = r_2 + (p - r_2) \in \alpha +_{\mathbb{R}} 0_{\mathbb{R}} \blacksquare p \in \alpha +_{\mathbb{R}} 0_{\mathbb{R}}$
- (1.5)  $p \in \alpha \implies p \in \alpha +_{\mathbb{R}} 0_{\mathbb{R}} \blacksquare \forall_{p \in \alpha} (p \in \alpha +_{\mathbb{R}} 0_{\mathbb{R}}) \blacksquare \alpha \subseteq \alpha +_{\mathbb{R}} 0_{\mathbb{R}}$
- (1.6)  $\alpha +_{\mathbb{R}} 0_{\mathbb{R}} \subseteq \alpha \wedge \alpha \subseteq \alpha +_{\mathbb{R}} 0_{\mathbb{R}} \blacksquare 0_{\mathbb{R}} +_{\mathbb{R}} \alpha = \alpha$
- (2)  $\alpha \in \mathbb{R} \implies 0_{\mathbb{R}} +_{\mathbb{R}} \alpha = \alpha$

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

- (1)  $\alpha \in \mathbb{R} \implies \dots$
- (1.1)  $\beta := \{p \in \mathbb{Q} : \exists_{r > 0} (-p - r \notin \alpha)\}$
- (1.2)  $\alpha \subset \mathbb{Q} \blacksquare \exists_{s \in \mathbb{Q}} (s \notin \alpha) \blacksquare s_0 := \text{choice}(\{s : s \notin \alpha\}) \blacksquare p_0 := -s_0 - 1$
- (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)  $\emptyset \neq \alpha \blacksquare \exists_{q \in \alpha} \blacksquare q_0 := \text{choice}(\{q \in \mathbb{Q} : q \in \alpha\})$
- (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)  $\emptyset \neq \beta \subset \mathbb{Q} \blacksquare \text{CutI}[\beta]$
- (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)	$p \in \beta \implies \exists_{r>0}(-p-r \notin \alpha) \blacksquare r_1 := \text{choice}(\{r > 0 : -p-r \notin \alpha\})$	
(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)	$\alpha \in \mathbb{R} \implies \exists_{-\alpha \in \mathbb{R}}(\alpha +_{\mathbb{R}} (-\alpha) = 0_{\mathbb{R}})$	

$*_{\mathbb{R}}[\alpha, \beta] := \text{---}$

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

$11sNot0 := 0_{\mathbb{R}} \neq 1_{\mathbb{R}} \text{ ---}$

$11nR := 1_{\mathbb{R}} \in \mathbb{R} \text{ ---}$

$\text{FieldMultiplicationClosureOf } \mathbb{R} := (\alpha, \beta \in \mathbb{R}) \implies ((\alpha *_{\mathbb{R}} \beta) \in \mathbb{R}) \text{ ---}$

$\text{FieldMultiplicationCommutativityOf } \mathbb{R} := (\alpha, \beta \in \mathbb{R}) \implies (\alpha *_{\mathbb{R}} \beta = \beta *_{\mathbb{R}} \alpha) \text{ ---}$

$\text{FieldMultiplicationAssociativityOf } \mathbb{R} := (\alpha, \beta, \gamma \in \mathbb{R}) \implies ((\alpha *_{\mathbb{R}} \beta) *_{\mathbb{R}} \gamma = \alpha *_{\mathbb{R}} (\beta *_{\mathbb{R}} \gamma)) \text{ ---}$

$\text{FieldMultiplicationIdentityOf } \mathbb{R} := (\alpha \in \mathbb{R}) \implies 1_{\mathbb{R}} *_{\mathbb{R}} \alpha = \alpha \text{ ---}$

$\text{FieldMultiplicationInverseOf } \mathbb{R} := (\alpha \in \mathbb{R}) \implies \exists_{1/\alpha \in \mathbb{R}}(\alpha *_{\mathbb{R}} (1/\alpha) = 1_{\mathbb{R}}) \text{ ---}$

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

$\text{FieldWith } \mathbb{R} := \text{Field}[\mathbb{R}, +_{\mathbb{R}}, *_{\mathbb{R}}] \text{ ---}$

$\text{OrderedFieldWith } \mathbb{R} := \text{OrderedField}[\mathbb{R}, +_{\mathbb{R}}, *_{\mathbb{R}}, <_{\mathbb{R}}] \text{ ---}$

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

$\text{QROrderedSubfieldOf } \mathbb{R} := \text{OrderedSubfield}[\mathbb{Q}_{\mathbb{R}}, \mathbb{R}, +_{\mathbb{R}}, *_{\mathbb{R}}, <_{\mathbb{R}}] \text{ ---}$

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

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

(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)  $\text{ArchimedeanPropertyOfR} \wedge (0 < y - x) \wedge (y - x, 1 \in \mathbb{R}) \blacksquare \exists_{n \in \mathbb{N}^+}(n(y - x) > 1) \dots$
- (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)  $\text{ArchimedeanPropertyOfR} \wedge (1 > 0) \wedge (n_0 x, 1 \in \mathbb{R}) \blacksquare \exists_{m \in \mathbb{N}^+}(m(1) > n_0 x) \dots$
- (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)  $\text{ArchimedeanPropertyOfR} \wedge (1 > 0) \wedge (-n_0 x, 1 \in \mathbb{R}) \blacksquare \exists_{m \in \mathbb{N}^+}(m(1) > -n_0 x) \dots$
- (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)  $b/a > 1 \blacksquare \sum_{i=1}^n (b^{n-i} a^{i-1}) \leq \sum_{i=1}^n (b^{n-i} a^{i-1} (b/a)^{i-1}) = \sum_{i=1}^n (b^{n-1}) = nb^{n-1} \blacksquare \sum_{i=1}^n (b^{n-i} a^{i-1}) \leq \sum_{i=1}^n (b^{n-1}) = nb^{n-1}$
- (1.4)  $b^n - a^n = (b - a) \sum_{i=1}^n (b^{n-i} a^{i-1}) \leq (b - a)nb^{n-1} \blacksquare b^n - a^n \leq (b - a)nb^{n-1}$
- (2)  $(0 < a < b) \implies (b^n - a^n \leq (b - a)nb^{n-1})$

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

- (1)  $(0 < x \in \mathbb{R} \wedge 0 < n \in \mathbb{Z}) \implies \dots$
- (1.1)  $E := \{t \in \mathbb{R} : t > 0 \wedge t^n < x\} \blacksquare t \in E \iff (t \in \mathbb{R} \wedge t > 0 \wedge t^n < x)$
- (1.2)  $t_0 := x/(1 + x) \blacksquare (t_0 = x/(1 + x)) \wedge (t_0 \in \mathbb{R})$
- (1.3)  $0 < x \blacksquare 0 < x < 1 + x \blacksquare t_0 = x/(1 + x) > 0 \blacksquare t_0 > 0$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(1.17) \quad \text{CompletenessOfR} \quad \blacksquare \quad \text{LUBProperty}[\mathbb{R}, <]$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(1.22) \quad y_0^n < x \implies \perp \quad \blacksquare \quad y_0^n \geq x$$

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

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

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

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

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

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

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

(1.23.7)	$(k_1 < y_0) \wedge (0 < k_1) \quad \blacksquare \quad (0 < k_1 < y_0) \wedge (0 < y_0 - k_1 < y_0)$	
(1.23.8)	$t \geq y_0 - k_1 \implies \dots$	
(1.23.8.1)	$t \geq y_0 - k_1 \quad \blacksquare \quad t^n \geq (y_0 - k_1)^n \quad \blacksquare \quad -t^n \leq -(y_0 - k_1)^n \quad \blacksquare \quad y_0^n - t^n \leq y_0^n - (y_0 - k_1)^n$	
(1.23.8.2)	$\textcolor{blue}{RootLemma} \wedge (0 < y_0 - k_1 < y_0) \quad \blacksquare \quad y_0^n - (y_0 - k_1)^n < k_1 n y_0^{n-1}$	
(1.23.8.3)	$(y_0^n - t^n \leq y_0^n - (y_0 - k_1)^n) \wedge (y_0^n - t^n < k_1 n y_0^{n-1}) \quad \blacksquare \quad y_0^n - t^n < k_1 n y_0^{n-1}$	
(1.23.8.4)	$(k_1 n y_0^{n-1} = y_0^n - x) \wedge (y_0^n - t^n < k_1 n y_0^{n-1}) \quad \blacksquare \quad y_0^n - t^n < y_0^n - x \quad \blacksquare \quad -t^n < -x \quad \blacksquare \quad t^n > x$	
(1.23.8.5)	$(t \in E \iff (t \in \mathbb{R} \wedge t > 0 \wedge t^n < x)) \wedge (t^n > x) \quad \blacksquare \quad t \notin E$	
(1.23.9)	$t \geq y_0 - k_1 \implies t \notin E \quad \blacksquare \quad t \in E \implies t < y_0 - k_1 \quad \blacksquare \quad \forall_{t \in E} (t \leq y_0 - k_1) \quad \blacksquare \quad \textcolor{blue}{UpperBound}[y_0 - k_1, E, \mathbb{R}, <]$	
(1.23.10)	$(\textcolor{blue}{LUB}[y_0, E, \mathbb{R}, <] \wedge (y_0 - k_1 < y_0)) \quad \blacksquare \quad \neg \textcolor{blue}{UpperBound}[y_0 - k_1, E, \mathbb{R}, <]$	
(1.23.11)	$(\textcolor{blue}{UpperBound}[y_0 - k_1, E, \mathbb{R}, <]) \wedge (\neg \textcolor{blue}{UpperBound}[y_0 - k_1, E, \mathbb{R}, <]) \quad \blacksquare \quad \perp$	
(1.24)	$y_0^n > x \implies \perp \quad \blacksquare \quad y_0^n \leq x$	
(1.25)	$\textcolor{blue}{Order}[\mathbb{R}, <] \quad \blacksquare \quad \textcolor{blue}{OrderTrichotomy}[\mathbb{R}, <]$	
(1.26)	$(\textcolor{blue}{OrderTrichotomy}[\mathbb{R}, <]) \wedge (y_0^n \geq x) \wedge (y_0^n \leq x) \quad \blacksquare \quad y_0^n = x$	
(1.27)	$(y_0^n = x) \wedge (y_0 \in \mathbb{R}) \quad \blacksquare \quad \exists_{y \in \mathbb{R}} (y^n = x)$	
(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)	$(\textcolor{blue}{OrderTrichotomy}[\mathbb{R}, <]) \wedge (y_1 \neq y_2) \quad \blacksquare \quad (y_1 < y_2) \vee (y_2 < y_1) \quad \dots$	
(1.29.2)	$\dots (x = y_1^n < y_2^n = x) \vee (x = y_2^n < y_1^n = x) \quad \blacksquare \quad (x < x) \vee (x > x) \quad \blacksquare \quad \perp \vee \perp \quad \blacksquare \quad \perp$	
(1.30)	$y_1 \neq y_2 \implies \perp \quad \blacksquare \quad y_1 = y_2 \quad \blacksquare \quad \forall_{a,b \in \mathbb{R}} ((a^n = x \wedge b^n = x) \implies a = b)$	
(1.31)	$(\exists_{y \in \mathbb{R}} (y^n = x)) \wedge (\forall_{a,b \in \mathbb{R}} ((a^n = x \wedge b^n = x) \implies a = b)) \quad \blacksquare \quad \exists!_{y \in \mathbb{R}} (y^n = x)$	
(2)	$(0 < x \in \mathbb{R} \wedge 0 < n \in \mathbb{Z}) \implies \exists!_{y \in \mathbb{R}} (y^n = x) \quad \blacksquare \quad \forall_{0 < x \in \mathbb{R}} \forall_{0 < n \in \mathbb{Z}} \exists!_{0 < y \in \mathbb{R}} (y_0^n = x)$	

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

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

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

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

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

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

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

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

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

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

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

$$\textcolor{red}{ConjugateProperties} := (w, z \in \mathbb{C}) \implies \dots \quad \text{---}$$

$$(1) \quad \overline{z + w} = \bar{z} + \bar{w}$$

$$(2) \quad \overline{z * w} = \bar{z} * \bar{w}$$

$$(3) \quad \textit{Re}(z) = (1/2)(z + \bar{z}) \wedge \textit{Im}(z) = (1/2)(z - \bar{z})$$

$$(4) \quad 0 \leq z * \bar{z} \in \mathbb{R}$$

$$\textcolor{red}{AbsoluteValueC}[|z|] = (z * \bar{z})^{1/2}$$

$$\textcolor{red}{AbsoluteValueProperties} := (z, w \in \mathbb{C}) \implies \dots \quad \text{---}$$

$$(1) \quad 123123$$



# Chapter 2

## Abstract Algebra

### 2.1 Functions

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

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

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

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

(1) TODO

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

(1) TODO

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

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

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

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

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

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

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

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

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

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

(1) TODO

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

(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

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

(1) TODO

---


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

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

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

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

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

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

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

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

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

---


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


---

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

---


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


---

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

---


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


---

## 2.3 Groups

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

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

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

---


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


---

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

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

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

---


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


---

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


---

$$(3.1) \quad \text{TODO}$$


---

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


---

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


---

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

---


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


---

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

---


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


---

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

---


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


---

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


---

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


---



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

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

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

## 2.4 Subgroups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(7) \quad (a \in H_1 \cap H_2) \implies \dots$$

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

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

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

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

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

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

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

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

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

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

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

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

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


---

## 2.5 Special Groups

### 2.5.1 Cyclic Group

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

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

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

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

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

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

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

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

$$(1) \quad \text{ExpModOrder} \quad \blacksquare \quad (g^s = e) \iff (g^s = g^0) \iff (s \equiv 0 \pmod{n}) \iff (\text{Divides}[n, s - 0]) \iff (\text{Divides}[n, s])$$


---

### 2.5.2 Symmetric and Alternating Groups

$SymmetricGroup[S_n, n] := S_n = \{\text{permutation of a set with } n \text{ elements}\}$   
 $SymmetricGroupOrder := o(S_n) = n!$   
 $SymmetricGroupAsDisjoinsCycles := \forall_{\sigma \in S_n} \exists_{\Sigma \subseteq S_n} ((DisjointCycles[\Sigma]) \wedge (\sigma = \prod(\sigma_i)))$   
 $SymmetricGroupAsTranspositions := \forall_{\sigma \in S_n} \exists_{\Sigma \subseteq S_n} ((Transpositions[\Sigma]) \wedge (\sigma = \prod(\sigma_i)))$   
 $vFunction[v(\sigma), \sigma, S_n] := v(\sigma) = n - |DisjointFullCycles[\Sigma]|$   
 $signFunction[sign(\sigma), \sigma, S_n] := sign(\sigma) = (-1)^{v(\sigma)}$   
 $EvenPermutation[\sigma, S_n] := sign(\sigma) = 1$   
 $OddPermutation[\sigma, S_n] := sign(\sigma) = -1$

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

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

### 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

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

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

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

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

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

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

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

(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)  $EqRel[\sim, G]$

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

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

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

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

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

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

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

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

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

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

- (1) *LagrangeTheorem* ■ Subgroups must have the order 1 or p ■ Subgroups are trivial
- (2) CyclicSubgroup of a non-identity element is G ■ Non-identity elements generates G

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

- (1) (*LagrangeTheorem*)  $\wedge$  (*SubgroupIntersection*)  $\wedge$  (*RelPrime*( $o(H)$ ,  $o(K)$ )) ■  $H \cap K = \{e\}$

## 2.7 Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(1.1) \quad \phi(g^n) = \phi(g) = \phi(g)^n \quad \text{■} \quad \phi(g^n) = \phi(g)^n$$

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

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

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

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

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

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

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

- (1)  $\text{OrderElDivOrder}$  ■  $g^n = e_G$

- (2)  $(\text{IdMapsId}) \wedge (\text{ExpMapsExp})$  ■  $e_H = \phi(e_G) = \phi(g^n) = \phi(g)^n$  ■  $\phi(g)^n = e_H$

- (3)  $(\text{ExpModOrderCorollary}) \wedge (\text{OrderEl}[m, \phi(g), H, \diamond]) \wedge (\phi(g)^n = e_H)$  ■  $\text{Divides}[m, n]$

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

- (1)  $\text{Inj}[\phi, G, H]$  ■  $\forall_{g_1, g_2 \in G} ((\phi(g_1) = \phi(g_2)) \implies (g_1 = g_2))$

- (2)  $e_H = \phi(g)^m = \phi(g^m)$  ■  $e_H = \phi(g^m)$

- (3)  $e_H = \phi(e_G) = \phi(g^n)$  ■  $e_H = \phi(g^n)$

- (4)  $(\forall_{g_1, g_2 \in G} ((\phi(g_1) = \phi(g_2)) \implies (g_1 = g_2))) \wedge (e_H = \phi(g^m)) \wedge (e_H = \phi(g^n))$  ■  $g^m = g^n$

- (5)  $(\text{OrderEl}[m, \phi(g), H, \diamond]) \wedge (\text{Order}[n, G, *]) \wedge (g^m = g^n)$  ■  $m = n$

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

- (1)  $\text{FuncComp}$  ■  $\text{Func}[\theta \circ \phi, G, K]$

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

- 
- (2.1)  $(Homomorphism[\phi, G, *, H, \diamond]) \wedge (Homomorphism[\theta, H, \diamond, K, \square]) \blacksquare \theta \circ \phi(g_1 * g_2) = \theta(\phi(g_1 * g_2)) = \dots$
- (2.2)  $\dots \theta(\phi(g_1) \diamond \phi(g_2)) = \theta(\phi(g_1)) \square \theta(\phi(g_2)) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2) \blacksquare \theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2)$
- 
- (3)  $(g_1, g_2 \in G) \implies (\theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2)) \blacksquare \forall_{g_1, g_2 \in G} (\theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2))$
- 
- (4)  $(Func[\theta \circ \phi, G, K]) \wedge (\forall_{g_1, g_2 \in G} (\theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2))) \blacksquare Homomorphism[\theta \circ \phi, G, *, K, \square]$
- 

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

- 
- (1)  $Isomorphism[\phi, G, *, H, \diamond] \blacksquare (Homomorphism[\phi, G, *, H, \diamond]) \wedge (Bij[\phi, G, H])$
- 
- (2)  $BijEquiv \blacksquare \exists_{\phi^{-1}}(Inv[\phi^{-1}, \phi, G, H]) \blacksquare Bij[\phi^{-1}, H, G]$
- 
- (3)  $(x, y \in H) \implies \dots$
- 
- (3.1)  $Homomorphism[\phi, G, *, H, \diamond] \blacksquare \phi(\phi^{-1}(x) * \phi^{-1}(y)) = \phi(\phi^{-1}(x)) \diamond \phi(\phi^{-1}(y)) = x \diamond y$
- 
- (3.2)  $\phi^{-1}(x \diamond y) = \phi^{-1}(\phi(\phi^{-1}(x) * \phi^{-1}(y))) = (\phi^{-1} \circ \phi)(\phi^{-1}(x) * \phi^{-1}(y)) = \phi^{-1}(x) * \phi^{-1}(y) \blacksquare \phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y)$
- 
- (4)  $(x, y \in H) \implies (\phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y)) \blacksquare \forall_{x, y \in H} (\phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y))$
- 
- (5)  $(Bij[\phi^{-1}, H, G]) \wedge (\forall_{x, y \in H} (\phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y))) \blacksquare Isomorphism[\phi^{-1}, H, \diamond, G, *]$
- 

$KCycleGroupIsomorphic := \left( ((CyclicGroup[G, *]) \wedge (CyclicGroup[H, \diamond]) \wedge (Order[n, G, *]) \wedge (Order[n, H, \diamond])) \implies \right. \\ \left. (Isomorphic[G, *, H, \diamond]) \right)$

- 
- (1)  $(\exists_{g \in G} (Generator[g, G, *])) \wedge (\exists_{h \in H} (Generator[h, H, \diamond]))$
- 
- (2)  $\phi := \{ \langle g^n, h^n \rangle \in (G \times H) \mid n \in \mathbb{Z} \}$
- 
- (3)  $(n_1, n_2 \in \mathbb{Z}) \implies \dots$
- 
- (3.1)  $(ExpModOrder) \wedge (Order[n, G, *]) \wedge (Order[n, H, \diamond]) \blacksquare (g^{n_1} = g^{n_2}) \iff (n_1 \equiv n_2 \pmod{n}) \iff (h^{n_1} = h^{n_2}) \iff \dots$
- 
- (3.2)  $\dots (\phi(g^{n_1}) = \phi(g^{n_2})) \blacksquare (g^{n_1} = g^{n_2}) \iff (\phi(g^{n_1}) = \phi(g^{n_2}))$
- 
- (4)  $(n_1, n_2 \in \mathbb{Z}) \implies ((g^{n_1} = g^{n_2}) \iff (\phi(g^{n_1}) = \phi(g^{n_2}))) \dots$
- 
- (5)  $\dots (Func[\phi, G, H]) \wedge (Inj[\phi, G, H]) \wedge (Surj[\phi, G, H]) \blacksquare Bij[\phi, G, H]$
- 
- (6)  $(g^n, g^m \in G) \implies \dots$
- 
- (6.1)  $\phi(g^n * g^m) = \phi(g^{n+m}) = h^{n+m} = h^n \diamond h^m = \phi(g^n) \diamond \phi(g^m) \blacksquare \phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m)$
- 
- (7)  $(g^n, g^m \in G) \implies (\phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m)) \blacksquare \forall_{g^n, g^m \in G} (\phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m))$
- 
- (8)  $(Bij[\phi, G, H]) \wedge (\forall_{g^n, g^m \in G} (\phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m))) \blacksquare Isomorphism[\phi, G, *, H, \diamond]$
- 
- (9)  $\exists_{\phi}(Isomorphism[\phi, G, *, H, \diamond]) \blacksquare Isomorphic[G, *, H, \diamond]$
- 

## 2.8 Kernel and Image Homomorphisms

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

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

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

- 
- (1)  $IdMapsId \blacksquare \phi(e_G) = e_H \blacksquare e_G \in ker_{\phi} \blacksquare ker_{\phi} \neq \emptyset$
- 
- (2)  $ker_{\phi} \subseteq G \blacksquare \emptyset \neq ker_{\phi} \subseteq G$
- 
- (3)  $(a, b \in ker_{\phi}) \implies \dots$
- 
- (3.1)  $(\phi(a) = e_H) \wedge (\phi(b) = e_H) \blacksquare \phi(a * b) = \phi(a) \diamond \phi(b) = e_H \diamond e_H = e_H \blacksquare a * b \in ker_{\phi}$
- 
- (4)  $(a, b \in ker_{\phi}) \implies (a * b \in ker_{\phi}) \blacksquare \forall_{a, b \in ker_{\phi}} (a * b \in ker_{\phi})$
- 
- (5)  $(a \in ker_{\phi}) \implies \dots$
- 
- (5.1)  $\phi(a) = e_H$
- 
- (5.2)  $InvMapsInv \blacksquare \phi(a^{-1}) = e_H^{-1} = e_H \blacksquare a^{-1} \in ker_{\phi}$
- 
- (6)  $(a \in ker_{\phi}) \implies (a^{-1} \in ker_{\phi}) \blacksquare \forall_{a \in ker_{\phi}} (a^{-1} \in ker_{\phi})$
- 
- (7)  $(SubgroupEquiv) \wedge (\emptyset \neq ker_{\phi} \subseteq G) \wedge (\forall_{a, b \in ker_{\phi}} (a * b \in ker_{\phi})) \wedge (\forall_{a \in ker_{\phi}} (a^{-1} \in ker_{\phi})) \blacksquare Subgroup[ker_{\phi}, G, *]$
- 

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

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

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

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

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

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

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

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

$$(5) \quad (a \in im_\phi) \implies \dots$$

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

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

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

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

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

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

$$(1) \quad CyclicGroup[G, *] \quad \blacksquare \quad \exists_{r \in G}(Generator[r, G, *]) \quad \blacksquare \quad G = \langle r \rangle = \{r^n \mid n \in \mathbb{Z}\}$$

$$(2) \quad ExpMapsExp \quad \blacksquare \quad im_\phi = \{\phi(g) \mid g \in G\} = \{\phi(r^n) \mid n \in \mathbb{Z}\} = \{\phi(r^n) \mid n \in \mathbb{Z}\} = \langle \phi(r) \rangle$$

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

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

$$(1) \quad (Inj[\phi, G, H]) \implies \dots$$

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

$$(1.2) \quad (g \in ker_\phi) \implies \dots$$

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

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

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

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

$$(2) \quad (Inj[\phi, G, H]) \implies (ker_\phi = \{e_G\})$$

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

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

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

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

$$(3.2) \quad ((g_1, g_2 \in G) \wedge (\phi(g_1) = \phi(g_2))) \implies (g_1 = g_2) \quad \blacksquare \quad \forall_{g_1, g_2 \in G}((\phi(g_1) = \phi(g_2)) \implies (g_1 = g_2)) \quad \blacksquare \quad Inj[\phi, G, H]$$

$$(4) \quad (ker_\phi = \{e_G\}) \implies (Inj[\phi, G, H])$$

$$(5) \quad ((Inj[\phi, G, H]) \implies (ker_\phi = \{e_G\})) \wedge ((ker_\phi = \{e_G\}) \implies (Inj[\phi, G, H]))$$

$$(6) \quad (Inj[\phi, G, H]) \iff (ker_\phi = \{e_G\})$$

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

$$(1) \quad (x \in (ker_\phi)g) \implies \dots$$

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

$$(2) \quad (x \in (ker_\phi)g) \implies (\phi(x) = \phi(g)) \quad \blacksquare \quad (ker_\phi)g \subseteq \{x \in G \mid \phi(x) = \phi(g)\}$$

$$(3) \quad ((x \in G) \wedge (\phi(x) = \phi(g))) \implies \dots$$

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

$$(4) \quad ((x \in G) \wedge (\phi(x) = \phi(g))) \implies (x \in (ker_\phi)g) \quad \blacksquare \quad \{x \in G \mid \phi(x) = \phi(g)\} \subseteq (ker_\phi)g$$

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

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

- (1)  $\forall_{g \in G} ([g] = \{x \in G \mid \phi(x) = \phi(g)\})$
- (2)  $\mathcal{G} = \{[g] \mid g \in G\} \quad \blacksquare \quad (Partition[\mathcal{G}, G]) \wedge (|\mathcal{G}| = |im_\phi|)$
- (3)  $KerMultiplicityMap \quad \blacksquare \quad \forall_{g \in G} (|[g]| = |ker_\phi|)$
- (4)  $Partition[\mathcal{G}, G] \quad \blacksquare \quad |G| = |\mathcal{G}| |ker_\phi| = |im_\phi| |ker_\phi|$

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

- (1)  $KerImPartitionsG \quad \blacksquare \quad |G| = |ker_\phi| |im_\phi| \quad \blacksquare \quad Divides[|im_\phi|, |G|]$
- (2)  $(LagrangeTheorem) \wedge (ImageSubgroupCodomain) \quad \blacksquare \quad |H| = |im_\phi| |H : im_\phi| \quad Divides[|im_\phi|, |H|]$

## 2.9 Conjugacy

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

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

- (1)  $(a, b, c \in G) \implies \dots$ 
  - (1.1)  $a = e^{-1} * a * e \quad \blacksquare \quad a \sim^* a$
  - (1.2)  $(a \sim^* b) \implies (b = x_b^{-1} * a * x_b) \implies (x_b * b * x_b^{-1} = a) \implies (b \sim^* a)$
  - (1.3)  $((a \sim^* b) \wedge (b \sim^* c)) \implies ((b = x_b^{-1} * a * x_b) \wedge (c = x_c^{-1} * b * x_c)) \implies \dots$
  - (1.4)  $\dots (c = x_c^{-1} * x_b^{-1} * a * x_b * x_c = (x_b * x_c)^{-1} * a * (x_b * x_c)) \quad \blacksquare \quad a \sim^* c$
- (2)  $EqRel[\sim^*, G]$

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

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

- (1) By ConjugateEqRel and the definitions of ConjugacyClass, Conjugate

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

- (1)  $(C_g = \{g\}) \implies \dots$ 
  - (1.1)  $(x \in G) \implies \dots$ 
    - (1.1.1)  $(ConjugacyClass[C_g, g, G, *]) \wedge (ConjugacyClassEquiv) \wedge (x \in G) \quad \blacksquare \quad x^{-1} g x \in C_g$
    - (1.1.2)  $(C_g = \{g\}) \wedge (x^{-1} g x \in C_g) \quad \blacksquare \quad x^{-1} g x = g \quad \blacksquare \quad g x = x g$
  - (1.2)  $(x \in G) \implies (g x = x g) \quad \blacksquare \quad \forall_{x \in G} (g x = x g) \quad \blacksquare \quad g \in Z(G)$
- (2)  $(C_g = \{g\}) \implies (g \in Z(G))$
- (3)  $(g \in Z(G)) \implies \dots$ 
  - (3.1)  $(g \in Z(G)) \wedge (Group[G, *]) \quad \blacksquare \quad (\forall_{c \in G} (g c = c g)) \wedge (\exists_e (e \in G))$
  - (3.2)  $(x \in G) \implies \dots$ 
    - (3.2.1)  $(\forall_{c \in G} (g c = c g)) \wedge (\exists_e (e \in G)) \quad \blacksquare \quad (\exists_{c \in G} (x = c^{-1} g c)) \iff (\exists_{c \in G} (x = c^{-1} g c = c^{-1} c g = g)) \iff (x = g) \iff (x \in \{g\})$
  - (3.3)  $(x \in G) \implies ((\exists_{c \in G} (x = c^{-1} g c)) \iff (x \in \{g\})) \quad \blacksquare \quad \forall_{x \in G} ((x \in \{g\}) \iff (\exists_{c \in G} (x = c^{-1} g c)))$
  - (3.4)  $(ConjugacyClassEquiv) \wedge (\forall_{x \in G} ((x \in \{g\}) \iff (\exists_{c \in G} (x = c^{-1} g c)))) \quad \blacksquare \quad C_g = \{g\}$
- (4)  $(g \in Z(G)) \implies (C_g = \{g\})$
- (5)  $(C_g = \{g\}) \iff (g \in Z(G))$

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

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

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

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

- 
- (2)  $(n = 1) \implies ((x^{-1}gx)^n = x^{-1}g^nx)$
- 
- (3)  $((n > 1) \wedge (\forall_{m \in \mathbb{N}^+} ((m \leq n) \implies ((x^{-1}gx)^m = x^{-1}g^mx)))) \implies \dots$
- 
- (3.1)  $(x^{-1}gx)^{n+1} = (x^{-1}gx)^n * (x^{-1}gx) = (x^{-1}g^nx) * (x^{-1}gx) = x^{-1}g^{n+1}x \blacksquare (x^{-1}gx)^{n+1} = x^{-1}g^{n+1}x$
- 
- (4)  $((n > 1) \wedge (\forall_{m \in \mathbb{N}^+} ((m \leq n) \implies ((x^{-1}gx)^m = x^{-1}g^mx)))) \implies ((x^{-1}gx)^{n+1} = x^{-1}g^{n+1}x)$
- 
- (5)  $\forall_{n \in \mathbb{N}^+} ((x^{-1}gx)^n = x^{-1}g^nx)$
- 

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

---

- (1)  $\exists_{c \in G} (g_2 = c^{-1}g_1c)$
- 
- (2) *ConjugateExp*  $\blacksquare e = g_2^{o(g_2)} = (c^{-1}g_1c)^{o(g_2)} = c^{-1}g_1^{o(g_2)}c \blacksquare e = c^{-1}g_1^{o(g_2)}c \blacksquare g_1^{o(g_2)} = e$
- 
- (3) *ExpModOrderCorollary*  $\blacksquare \text{Divides}[o(g_2), o(g_1)]$
- 
- (4) *ConjugateExp*  $\blacksquare e = g_1^{o(g_1)} = (cg_2c^{-1})^{o(g_1)} = cg_2^{o(g_1)}c^{-1} \blacksquare e = cg_2^{o(g_1)}c^{-1} \blacksquare g_2^{o(g_1)} = e$
- 
- (5) *ExpModOrderCorollary*  $\blacksquare \text{Divides}[o(g_1), o(g_2)]$
- 
- (6)  $(\text{Divides}[o(g_2), o(g_1)]) \wedge (\text{Divides}[o(g_1), o(g_2)]) \wedge (g_1, g_2 \in \mathbb{N}^+) \blacksquare o(g_1) = o(g_2)$
- 
- (7) =====
- 
- (8)  $\exists_{c \in G} (g_2 = c^{-1}g_1c) \blacksquare e = g_2^{o(g_2)} = (c^{-1}g_1c)^{o(g_2)} = c^{-1}g_1^{o(g_2)}c \blacksquare e = c^{-1}g_1^{o(g_2)}c \blacksquare g_1^{o(g_2)} = e$
- 
- (9)  $(m \in \mathbb{Z}^+) \wedge (m < o(g_2)) \implies \dots$
- 
- (9.1)  $e \neq g_2^m = (c^{-1}g_1c)^m = c^{-1}g_1^mc \blacksquare e \neq c^{-1}g_1^mc \blacksquare e = c * e * c^{-1} \neq g_1^m \blacksquare g_1^m \neq e$
- 
- (10)  $(m < o(g_2)) \implies (e \neq g_1^m) \blacksquare \forall_{m \in \mathbb{Z}^+} ((m < o(g_2)) \implies (g_1^m \neq e))$
- 
- (11)  $(g_1^{o(g_2)} = e) \wedge (\forall_{m \in \mathbb{Z}^+} ((m < o(g_2)) \implies (g_1^m \neq e))) \blacksquare o(g_1) = o(g_2)$
- 

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

---

- (1)  $(c^{-1}ac \in c^{-1}C(g)c) \implies \dots$
- 
- (1.1)  $a \in C(g) \blacksquare ag = ga$
- 
- (1.2)  $(c^{-1}ac)h = (c^{-1}ac)(c^{-1}gc) = c^{-1}agc = c^{-1}gac = c^{-1}g(cc^{-1})ac = h(c^{-1}ac) \blacksquare (c^{-1}ac)h = h(c^{-1}ac) \blacksquare c^{-1}ac \in C(h)$
- 
- (2)  $(c^{-1}ac \in c^{-1}C(g)c) \implies (c^{-1}ac \in C(h)) \blacksquare c^{-1}C(g)c \subseteq C(h)$
- 
- (3)  $(a \in C(h)) \implies \dots$
- 
- (3.1)  $a \in C(h) \blacksquare ah = ha \blacksquare a(c^{-1}gc) = (c^{-1}gc)a$
- 
- (3.2)  $(cac^{-1})g = g(cac^{-1}) \blacksquare cac^{-1} \in C(g) \blacksquare a \in c^{-1}C(g)c$
- 
- (4)  $(a \in C(h)) \implies (a \in c^{-1}C(g)c) \blacksquare C(h) \subseteq c^{-1}C(g)c$
- 
- (5)  $(c^{-1}C(g)c \subseteq C(h)) \wedge (C(h) \subseteq c^{-1}C(g)c) \blacksquare C(h) = c^{-1}C(g)c$
- 

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

---

- (1)  $\phi := \{ \langle a^{-1}ga, C(g)a \rangle \in (C_g \times G : C(g)) \mid a \in G \}$
- 
- (2)  $(x, y \in G) \implies \dots$
- 
- (2.1)  $(x^{-1}gx = y^{-1}gy) \iff (gx = xy^{-1}gy) \iff (g(xy^{-1}) = (xy^{-1})g) \iff \dots$
- 
- (2.2)  $\dots (xy^{-1} \in C(g)) \iff (C(g)(xy^{-1}) = C(g)) \iff (C(g)x = C(g)y)$
- 
- (3)  $(x, y \in G) \implies ((x^{-1}gx = y^{-1}gy) \iff (C(g)x = C(g)y)) \dots$
- 
- (4)  $\dots (\text{Func}[\phi, C_g, G : C(g)]) \wedge (\text{Inj}[\phi, C_g, G : C(g)]) \wedge (\text{Surj}[\phi, C_g, G : C(g)]) \blacksquare \text{Bij}[\phi, C_g, G : C(g)]$
- 
- (5)  $\exists_{\phi} (\text{Bij}[\phi, C_g, G : C(g)]) \blacksquare |C_g| = |G : C(g)|$
- 
- (6)  $(\text{LagrangeTheorem}) \wedge (\text{SubgroupCenter}) \wedge (|C_g| = |G : C(g)|) \blacksquare o(G) = o(C(g))|G : C(g)| \blacksquare o(G) = o(C(g))|C_g|$
- 

## 2.10 Normal Subgroups

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

---

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

---

- (1) *SubgroupCenter*  $\blacksquare \text{Subgroup}[Z(G), G, *]$
- 
- (2)  $((h \in Z(G)) \wedge (g \in G)) \implies \dots$
-



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

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

---

- (1)  $(\text{NormalSubgroup}[H, G, *]) \implies \dots$
- (1.1)  $\text{NormalSubgroup}[H, G, *] \quad \blacksquare \quad \forall_{x \in H} \forall_{g \in G} (g^{-1}xg \in H)$
- (1.2)  $((x \in H) \wedge (y \in C_x)) \implies \dots$
- (1.2.1)  $\text{ConjugacyClassEquiv} \quad \blacksquare \quad \exists_{c \in G} (y = c^{-1}xc)$
- (1.2.2)  $(\forall_{x \in H} \forall_{g \in G} (g^{-1}xg \in H)) \wedge (x \in H) \wedge (c \in G) \quad \blacksquare \quad y \in H$
- (1.3)  $((x \in H) \wedge (y \in C_x)) \implies (y \in H) \quad \blacksquare \quad \forall_{x \in H} (C_x \subseteq H)$
- (1.4)  $\forall_{x \in H} (C_x \subseteq H) \quad \blacksquare \quad \forall_{x \in H} \forall_y (y \in C_x \implies y \in H) \quad \blacksquare \quad \forall_{x \in H} \forall_y (y \notin H \implies y \notin C_x)$
- (1.5)  $(b \in H) \implies (b \in C_b \subseteq \bigcup_{z \in H} (C_z)) \quad \blacksquare \quad (b \in H) \implies (b \in \bigcup_{z \in H} (C_z))$
- (1.6)  $(b \notin H) \implies (\forall_{a \in H} (b \notin C_a)) \implies (b \notin \bigcup_{z \in H} (C_z)) \quad \blacksquare \quad (b \notin H) \implies (b \notin \bigcup_{z \in H} (C_z))$
- (1.7)  $((b \in H) \implies (b \in \bigcup_{z \in H} (C_z))) \wedge ((b \notin H) \implies (b \notin \bigcup_{z \in H} (C_z))) \quad \blacksquare \quad (b \in H) \iff (b \in \bigcup_{z \in H} (C_z))$
- (1.8)  $\forall_b ((b \in H) \iff (b \in \bigcup_{z \in H} (C_z))) \quad \blacksquare \quad H = \bigcup_{z \in H} (C_z)$
- (2)  $(\text{NormalSubgroup}[H, G, *]) \implies (H = \bigcup_{z \in H} (C_z))$
- 

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

---

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

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

---

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

$\text{KerInduceNormalSubgroup} := (\text{Homomorphism}[\phi, G, *, H, \diamond]) \implies (\text{NormalSubgroup}[\ker \phi, G, *])$

---

- (1)  $\text{KernelSubgroupDomain} \quad \blacksquare \quad \text{Subgroup}[\ker \phi, G, *]$
- (2)  $((h \in \ker \phi) \wedge (g \in G)) \implies \dots$
- (2.1)  $h \in \ker \phi \quad \blacksquare \quad \phi(h) = e_H$
- (2.2)  $(\text{Homomorphism}[\phi, G, *, H, \diamond]) \wedge (\text{InvMapsInv}) \quad \blacksquare \quad \phi(g^{-1} * h * g) = \phi(g^{-1}) \diamond \phi(h) \diamond \phi(g) = \phi(g)^{-1} \diamond e_H \diamond \phi(g) = e_H$
- (2.3)  $\phi(g^{-1} * h * g) = e_H \quad \blacksquare \quad g^{-1}hg \in \ker \phi$
- (3)  $((h \in \ker \phi) \wedge (g \in G)) \implies (g^{-1}hg \in \ker \phi) \quad \blacksquare \quad \forall_{h \in \ker \phi} \forall_{g \in G} (g^{-1}hg \in \ker \phi)$
- (4)  $(\text{Subgroup}[\ker \phi, G, *]) \wedge (\forall_{h \in \ker \phi} \forall_{g \in G} (g^{-1}hg \in \ker \phi)) \quad \blacksquare \quad \text{NormalSubgroup}[\ker \phi, G, *]$
- 

## 2.11 Quotient Groups

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

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

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

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

---

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

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

(1.2)	$(NormalSubgroup[H, G, *]) \wedge (x^{-1} \in G) \wedge (h_2 \in H) \quad \blacksquare \quad (x^{-1})^{-1}h_2x^{-1} = xh_2x^{-1} \in H$
(1.3)	$(Group[H, *]) \wedge (h_1, xh_2x^{-1} \in H) \quad \blacksquare \quad h_1xh_2x^{-1} \in H$
(1.4)	$(h_1xh_2x^{-1})(xy) = h_1xh_2y = z \quad \blacksquare \quad (h_1xh_2x^{-1})(xy) = z$
(1.5)	$(h_1xh_2x^{-1} \in H) \wedge ((h_1xh_2x^{-1})(xy) = z) \quad \blacksquare \quad \exists_{h_3 \in H} (z = h_3xy)$
(2)	$(\exists_{h_1, h_2 \in H} (z = h_1xh_2y)) \implies (\exists_{h_3 \in H} (z = h_3xy))$
(3)	$(\exists_{h_3 \in H} (z = h_3xy)) \implies \dots$
(3.1)	$(NormalSubgroup[H, G, *]) \wedge (x \in G) \wedge (h_3 \in H) \quad \blacksquare \quad x^{-1}h_3x \in H$
(3.2)	$Group[H, *] \quad \blacksquare \quad e \in H$
(3.3)	$(e)x(x^{-1}h_3x)y = h_3xy = z \quad \blacksquare \quad (e)x(x^{-1}h_3x)y = z$
(3.4)	$(x^{-1}h_3x, e \in H) \wedge ((e)x(x^{-1}h_3x)y = h_3xy = z) \quad \blacksquare \quad \exists_{h_1, h_2 \in H} (z = h_1xh_2y)$
(4)	$(\exists_{h_3 \in H} (z = h_3xy)) \implies (\exists_{h_1, h_2 \in H} (z = h_1xh_2y))$
(5)	$((\exists_{h_1, h_2 \in H} (z = h_1xh_2y)) \implies (\exists_{h_3 \in H} (z = h_3xy))) \wedge ((\exists_{h_3 \in H} (z = h_3xy)) \implies (\exists_{h_1, h_2 \in H} (z = h_1xh_2y)))$
(6)	$(\exists_{h_1, h_2 \in H} (z = h_1xh_2y)) \iff (\exists_{h_3 \in H} (z = h_3xy))$

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

(1)	$(Hx, Hy \in G/H) \implies \dots$
(1.1)	$(NormalSubgroup[H, G, *]) \wedge (QuotientGroupLemma) \quad \blacksquare \quad \forall_{x, y, z \in G} ((\exists_{h_1, h_2 \in H} (z = h_1xh_2y)) \iff (\exists_{h_3 \in H} (z = h_3xy)))$
(1.2)	$(z \in Hx \bar{*} Hy) \iff (\exists_{h_1, h_2 \in H} (z = h_1xh_2y)) \iff (\exists_{h_3 \in H} (z = h_3xy)) \iff (z \in Hxy) \quad \blacksquare \quad Hx \bar{*} Hy = Hxy$
(1.3)	$(Group[G, *]) \wedge (x, y \in G) \quad \blacksquare \quad xy \in G \quad \blacksquare \quad Hxy \in G/H$
(1.4)	$(Hx \bar{*} Hy = Hxy) \wedge (Hxy \in G/H) \quad \blacksquare \quad \exists!_{Hxy \in G/H} (Hx \bar{*} Hy = Hxy)$
(2)	$(Hx, Hy \in G/H) \implies (\exists!_{Hxy \in G/H} (Hx \bar{*} Hy = Hxy)) \quad \blacksquare \quad Func[\bar{*}, G/H, G/H]$
(3)	$(Hx, Hy, Hz \in G/H) \implies \dots$
(3.1)	$(Hx \bar{*} Hy) \bar{*} Hz = Hxy \bar{*} Hz = Hxyz = Hx \bar{*} Hyz = Hx \bar{*} (Hy \bar{*} Hz) \quad \blacksquare \quad (Hx \bar{*} Hy) \bar{*} Hz = Hx \bar{*} (Hy \bar{*} Hz)$
(4)	$(Hx, Hy, Hz \in G/H) \implies ((Hx \bar{*} Hy) \bar{*} Hz = Hx \bar{*} (Hy \bar{*} Hz)) \quad \blacksquare \quad \forall_{a, b, c \in G/H} ((a \bar{*} b) \bar{*} c = a \bar{*} (b \bar{*} c))$
(5)	$(He \in G/H) \wedge (\forall_{Hx \in G/H} (Hx \bar{*} He = Hxe = Hx = Hxe = He \bar{*} Hx)) \quad \blacksquare \quad \exists_{e \in G/H} \forall_{a \in G/H} (a \bar{*} e = a = e \bar{*} a)$
(6)	$(Hx \in G/H) \implies \dots$
(6.1)	$x \in G \quad \blacksquare \quad x^{-1} \in G \quad \blacksquare \quad Hx^{-1} \in G/H$
(6.2)	$Hx \bar{*} Hx^{-1} = Hxx^{-1} = He = Hx^{-1}x = Hx^{-1} \bar{*} Hx \quad \blacksquare \quad Hx \bar{*} Hx^{-1} = He = Hx^{-1} \bar{*} Hx$
(6.3)	$(Hx^{-1} \in G/H) \wedge (Hx \bar{*} Hx^{-1} = He = Hx^{-1} \bar{*} Hx) \quad \blacksquare \quad \exists_{Hx^{-1} \in G/H} (Hx \bar{*} Hx^{-1} = He = Hx^{-1} \bar{*} Hx)$
(7)	$(Hx \in G/H) \implies (\exists_{Hx^{-1} \in G/H} (Hx \bar{*} Hx^{-1} = He = Hx^{-1} \bar{*} Hx)) \quad \blacksquare \quad \forall_{a \in G/H} \exists_{a^{-1} \in G/H} (a \bar{*} a^{-1} = e = a^{-1} \bar{*} a)$
(8)	$(Func[\bar{*}, G/H, G/H]) \wedge (\forall_{a, b, c \in G/H} ((a \bar{*} b) \bar{*} c = a \bar{*} (b \bar{*} c))) \wedge (\exists_{e \in G/H} \forall_{a \in G/H} (a \bar{*} e = a = e \bar{*} a)) \wedge \dots$
(9)	$\dots (\forall_{a \in G/H} \exists_{a^{-1} \in G/H} (a \bar{*} a^{-1} = e = a^{-1} \bar{*} a)) \quad \blacksquare \quad Group[G/H, \bar{*}]$

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

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

(1)	$NaturalMap[\bar{\phi}, H, G, *] \quad \blacksquare \quad Func[\bar{\phi}, G, *, G/H, \bar{*}]$
(2)	$(x, y \in G) \implies \dots$
(2.1)	$\bar{\phi}(x * y) = Hxy = Hx \bar{*} Hy = \bar{\phi}(x) \bar{*} \bar{\phi}(y) \quad \blacksquare \quad \bar{\phi}(x * y) = \bar{\phi}(x) \bar{*} \bar{\phi}(y)$
(3)	$(x, y \in G) \implies (\bar{\phi}(x * y) = \bar{\phi}(x) \bar{*} \bar{\phi}(y)) \quad \blacksquare \quad \forall_{x, y \in G} (\bar{\phi}(x) \bar{*} \bar{\phi}(y))$
(4)	$(Func[\bar{\phi}, G, *, G/H, \bar{*}]) \wedge (\forall_{x, y \in G} (\bar{\phi}(x) \bar{*} \bar{\phi}(y))) \quad \blacksquare \quad Homomorphism[\bar{\phi}, G, *, G/H, \bar{*}]$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(1) \quad \text{Second IsoLemma} \quad \blacksquare (\text{Group}[(HN)/N, \bar{*}]) \wedge (\text{Group}[H/(H \cap N), \bar{*}])$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(13) \quad (\ker_\phi = H/K) \wedge (\text{im}_\phi = G/H) \wedge (\text{Isomorphic}[(G/K)/\ker_\phi, \bar{*}, \text{im}_\phi, \bar{*}]) \quad \blacksquare \text{Isomorphic}[(G/K)/(H/K), \bar{*}, G/H, \bar{*}]$$

# Chapter 3

## Linear Algebra

### 3.1 Matrix Operations and Special Matrices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

---

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

---

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

---

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

---

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

---

(2)  $A + O_1 = A = A + O_2 \implies O_1 = O_2$

---

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

---

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

---

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

---

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

---

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

---

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

---

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- (1)  $B := (1/2) * (A + A^T) ; C := (1/2) * (A - A^T)$
- (2)  $SymGen[B] \wedge SkewSymGen[C]$
- (3)  $A = (1/2) * (A + A^T) + (1/2) * (A - A^T) = B + C$
- (4)  $(1/2) * (A_1 + A_1^T) = (1/2) * (A_2 + A_2^T) \blacksquare A_1 = A_2$
- (5)  $(1/2) * (A_3 - A_3^T) = (1/2) * (A_4 - A_4^T) \blacksquare A_3 = A_4$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- (1)  $u_0 := O ; u_1 := choice(\{X \in \mathcal{M} \mid X \neq O\}) ; k := choice(\mathbb{R})$
- (2)  $TrivSol[u_0, A]$
- (3)  $(NonTrivSol[u_1, A]) \implies (Sol[u_1 + ku_0])$
- (4)  $(TrivSol[\vec{X}, A]) \implies (TrivSol[LC(\vec{X}), A])$

$$ElemMat[E] := (E = Swap(I_n, i, j)) \vee (Scale_*(I_n, i, c)) \vee (Combine_*(I_n, i, c, j))$$

$$ElemMatProd[E^*] := \exists_{\langle E \rangle} (\forall_{E_i \in E^*} (ElemMat[E_i]) \wedge (E^* = \prod_{E_i \in E^*} (E_i)))$$

$$RowEquiv[A, B] := \exists_{E^*} ((ElemMatProd[E^*]) \wedge (B = E^* * A))$$

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

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

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

- (1)  $TODO$

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

- (1)  $\exists_{E^*: ElemMatProd[E^*]} ([CD] = E^* * [AB])$
- (2)  $(E^* * A = C) \wedge (E^* * B = D)$
- (3)  $Sol[Y, A, B] \implies \dots$

- 
- (3.1)  $A * Y = B$
- 
- (3.2)  $C * Y = (E^* * A) * Y = E^* * (A * Y) = E^* * B = D \quad \blacksquare \text{ Sol}[Y, C, D]$
- 
- (4)  $\text{Sol}[Y, A, B] \implies \text{Sol}[Y, C, D]$
- 
- (5)  $(A = (E^*)^{-1} * C) \wedge (B = (E^*)^{-1} * D)$
- 
- (6)  $\text{Sol}[Z, C, D] \implies \dots$
- 
- (6.1)  $C * Z = D$
- 
- (6.2)  $A * Z = ((E^*)^{-1} * C) * Z = (E^*)^{-1} * (C * Z) = (E^*)^{-1} * D = B$
- 
- (7)  $\text{Sol}[Z, C, D] \implies \text{Sol}[Z, A, B]$
- 
- (8)  $\text{Sol}[X, A, B] \iff \text{Sol}[X, C, D]$
- 

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

- 
- (1) Set  $B = D = O$
- 

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

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

- 
- (1) Hit  $A$  with  $\text{ElemMat}$ 's until it becomes  $B$
- 
- (2)  $(B = E^* * A) \wedge (\text{RREF}[B])$
- 

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

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

- 
- (1)  $i := \text{choice}(\{i \leq m \mid A_{i,:} = O\})$
- 
- (2)  $(B \in \mathcal{M}) \implies \dots$
- 
- (2.1)  $(A * B)_{i,:} = O \neq I_{n i,:} \quad \blacksquare \quad A * B \neq I_n$
- 
- (3)  $(B \in \mathcal{M}) \implies (A * B \neq I_n) \quad \blacksquare \quad \forall_{B \in \mathcal{M}} (A * B \neq I_n) \quad \blacksquare \quad \neg \text{Invertible}[A]$
- 

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

- 
- (1)  $(\text{Invertible}[A]) \implies \dots$
- 
- (1.1)  $(\text{RREF}[B]) \wedge (\text{RowEquiv}[A, B])$
- 
- (1.2)  $B = E^* * A$
- 
- (1.3)  $(\text{Invertible}[E^*]) \wedge (\text{Invertible}[A]) \quad \blacksquare \quad \text{Invertible}[B]$
- 
- (1.4)  $\text{Invertible}[B] \quad \blacksquare \quad \neg \text{HasZero}[B]$
- 
- (1.5)  $(\text{RREF}[B]) \wedge (\neg \text{HasZero}[B]) \quad \blacksquare \quad B = I_n$
- 
- (1.6)  $\text{RowEquiv}[A, I_n]$
- 
- (2)  $(\text{Invertible}[A]) \implies (\text{RowEquiv}[A, I_n])$
- 
- (3)  $(\text{RowEquiv}[A, I_n]) \implies \dots$
- 
- (3.1)  $I_n = E^* * A \quad \blacksquare \quad (E^*)^{-1} = A$
- 
- (3.2)  $A^{-1} = E^*_{\text{DescSort}} \quad \blacksquare \quad \text{Invertible}[A]$
- 
- (4)  $(\text{RowEquiv}[A, I_n]) \implies (\text{Invertible}[A])$
- 
- (5)  $(\text{Invertible}[A]) \iff (\text{RowEquiv}[A, I_n])$
- 

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

- 
- (1)  $(\text{RowEquiv}[A, I_n]) \implies \dots$
- 
- (1.1)  $\text{RowEquiv}[A, I_n] \quad \blacksquare \quad \text{Invertible}[A]$
- 
- (1.2)  $(\text{Sol}[X, A, O]) \implies \dots$
- 
- (1.2.1)  $A * X = O \quad \blacksquare \quad X = A^{-1} * O = O \quad \blacksquare \quad X = O$
- 
- (1.3)  $(\text{Sol}[X, A, O]) \implies (X = O)$
- 
- (1.4)  $(X = O) \implies (\text{Sol}[X, A, O])$
-



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

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

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

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

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

$$(3.3) \quad (B \neq I_n) \implies \dots$$

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

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

$$(3.3.3) \quad (Y \neq X) \wedge (Y = X) \quad \blacksquare \quad \perp$$

$$(3.4) \quad (B \neq I_n) \implies \perp \quad \blacksquare \quad B = I_n$$

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

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

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

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

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

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

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

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

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

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

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

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

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

### 3.3 Vector Spaces

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(2) \quad (r * v = O) \implies \dots$$

$$(2.1) \quad (r \neq 0) \implies \dots$$

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

$$(2.1.2) \quad ZeroVectorGenRight \quad \blacksquare \quad O = r^{-1} * O = r^{-1} * (r * v) = (r^{-1}r) * v = 1 * v = v \quad \blacksquare \quad O = v$$

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

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

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

### 3.4 Subspaces and Special Subspaces

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

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

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

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

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

$$(1.3) \quad (\emptyset \neq S) \wedge (S \subseteq V) \quad \blacksquare \quad \emptyset \neq S \subseteq V$$

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

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

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

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

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

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

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

$$(3.1.3) \quad u, v \in V \quad \blacksquare \quad u + v = v + u$$

$$(3.1.4) \quad u, v, w \in V \quad \blacksquare \quad (u + v) + w = u + (v + w)$$

$$(3.1.5) \quad u \in V \quad \blacksquare \quad u + O = u$$

$$(3.1.6) \quad (AddInvGen) \wedge (u \in S) \quad \blacksquare \quad (-1) * u = -u \in S$$

$$(3.1.7) \quad u \in V \quad \blacksquare \quad \alpha * (\beta * u) = (\alpha\beta) * u$$

$$(3.1.8) \quad u \in V \quad \blacksquare \quad 1 * u = u$$

$$(3.1.9) \quad u, v \in V \quad \blacksquare \quad \alpha * (u + v) = (\alpha * u) + (\alpha * v)$$

$$(3.1.10) \quad u \in V \quad \blacksquare \quad (\alpha + \beta) * u = (\alpha * u) + (\beta * u)$$

$$(4) \quad ((\emptyset \neq S) \wedge (\forall_{r, s \in S} (r + s \in S)) \wedge (\forall_{\alpha \in \mathbb{R}} \forall_{s \in S} (\alpha * s \in S))) \implies (Subspace[S, V, +, *])$$

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

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

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

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

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

$$(3) \quad (v \in A + B) \implies \dots$$

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

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

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

- (4)  $(v \in A + B) \implies (v \in V) \blacksquare A + B \subseteq V$
- (5)  $(\emptyset \neq A + B) \wedge (A + B \subseteq V) \blacksquare \emptyset \neq A + B \subseteq V$
- (6)  $(u, v \in A + B) \implies \dots$
- (6.1)  $(\exists_{a_1 \in A} \exists_{b_1 \in B} (u = a_1 + b_1)) \wedge (\exists_{a_2 \in A} \exists_{b_2 \in B} (v = a_2 + b_2))$
- (6.2)  $u + v = (a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2)$
- (6.3)  $(a_1 + a_2 \in A) \wedge (b_1 + b_2 \in B) \blacksquare u + v \in A + B$
- (7)  $(u, v \in A + B) \implies (u + v \in A + B) \blacksquare \forall_{u, v \in A + B} (u + v \in A + B)$
- (8)  $((r \in \mathbb{R}) \wedge (v \in A + B)) \implies \dots$
- (8.1)  $\exists_{a \in A} \exists_{b \in B} (v = a + b)$
- (8.2)  $r * v = r * (a + b) = r * a + r * b$
- (8.3)  $(r * a \in A) \wedge (r * b \in B) \blacksquare r * v \in A + B$
- (9)  $((r \in \mathbb{R}) \wedge (v \in A + B)) \implies (r * v \in A + B) \blacksquare \forall_{r \in \mathbb{R}} \forall_{v \in A + B} (r * v \in A + B)$
- (10)  $(SubspaceEquiv) \wedge (\emptyset \neq A + B \subseteq V) \wedge (\forall_{u, v \in A + B} (u + v \in A + B)) \wedge (\forall_{r \in \mathbb{R}} \forall_{v \in A + B} (r * v \in A + B)) \blacksquare Subspace[A + B, V, +, *]$
- (11)  $(O \in B) \wedge (\forall_{a \in A} (a + O) = a) \blacksquare A \subseteq A + B$
- (12)  $(O \in A) \wedge (\forall_{b \in B} (b + O) = b) \blacksquare B \subseteq A + B$
- (13)  $(A \subseteq A + B) \wedge (B \subseteq A + B) \blacksquare A, B \subseteq A + B$
- (14)  $(Subspace[A + B, V, +, *]) \wedge (A, B \subseteq A + B)$

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

- (1)  $SumSub \blacksquare (A, B \subseteq A + B) \wedge (Subspace[A + B, V, +, *])$
- (2)  $((Subspace[C, V, +, *]) \wedge (A, B \subseteq C)) \implies \dots$
- (2.1)  $(s \in A + B) \implies \dots$
- (2.1.1)  $\exists_{a \in A} \exists_{b \in B} (s = a + b)$
- (2.1.2)  $(A, B \subseteq C) \blacksquare a, b \in C$
- (2.1.3)  $(VectorSpace[C, V, +, *]) \wedge (a, b \in C) \blacksquare s = a + b \in C$
- (2.2)  $(s \in A + B) \implies (s \in C) \blacksquare A + B \subseteq C$
- (3)  $((Subspace[C, V, +, *]) \wedge (A, B \subseteq C)) \implies (A + B \subseteq C)$

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

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

- (1)  $(DirSum[A \oplus B, A, B, V, +, *]) \implies \dots$
- (1.1)  $(Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *]) \blacksquare (O \in A) \wedge (O \in B)$
- (1.2)  $(SubSum[A \oplus B, A, B, V, +, *]) \wedge (O \in A) \wedge (O \in B) \blacksquare O = O + O \in A \oplus B$
- (1.3)  $(DirSum[A \oplus B, A, B, V, +, *]) \wedge (O \in A \oplus B) \blacksquare \exists!_{\langle a, b \rangle \in A \times B} (O = a + b)$
- (2)  $(DirSum[A \oplus B, A, B, V, +, *]) \implies (\exists!_{\langle a, b \rangle \in A \times B} (O = a + b))$
- (3)  $(\exists!_{\langle a, b \rangle \in A \times B} (O = a + b)) \implies \dots$
- (3.1)  $(s \in A \oplus B) \implies \dots$
- (3.1.1)  $(\exists_{\langle a, b \rangle \in A \times B} (s = a + b))$
- (3.1.2)  $((s = a_1 + b_1) \wedge (s = a_2 + b_2)) \implies \dots$
- (3.1.2.1)  $O = s - s = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$
- (3.1.2.2)  $(Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *]) \blacksquare (a_1 - a_2 \in A) \wedge (b_1 - b_2 \in B)$
- (3.1.2.3)  $((a_1 - a_2 \neq O) \vee (b_1 - b_2 \neq O)) \implies (\neg \exists!_{\langle a, b \rangle \in A \times B} (O = a + b)) \implies \perp$
- (3.1.2.4)  $(a_1 - a_2 = O) \wedge (b_1 - b_2 = O) \blacksquare \langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle$
- (3.1.3)  $((s = a_1 + b_1) \wedge (s = a_2 + b_2)) \implies \langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle$
- (3.1.4)  $\forall_{\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \in A \times B} (((s = a_1 + b_1) \wedge (s = a_2 + b_2)) \implies (\langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle))$
- (3.1.5)  $\exists_{\langle a, b \rangle \in A \times B} (s = a + b) \wedge \forall_{\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \in A \times B} (((s = a_1 + b_1) \wedge (s = a_2 + b_2)) \implies (\langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle)) \blacksquare \exists!_{\langle a, b \rangle \in A \times B} (s = a + b)$
- (3.2)  $(s \in A + B) \implies \exists!_{\langle a, b \rangle \in A \times B} (s = a + b) \blacksquare \forall_{s \in A + B} \exists!_{\langle a, b \rangle \in A \times B} (s = a + b) \blacksquare DirSum[A \oplus B, A, B, V, +, *]$

$$(4) \quad (\exists!_{\langle a,b \rangle \in A \times B} (O = a + b)) \implies (DirSum[A \oplus B, A, B, V, +, *])$$

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

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

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

$$(1.1) \quad (v \in A \cap B) \implies \dots$$

$$(1.1.1) \quad (v \in A \cap B) \wedge (VectorSpace[B, +, *]) \blacksquare (v \in A) \wedge (v \in B) \blacksquare (v \in A) \wedge (-v \in B)$$

$$(1.1.2) \quad (v \in A) \wedge (-v \in B) \blacksquare v + (-v) = O \in A + B$$

$$(1.1.3) \quad DirSum[A \oplus B, A, B, V, +, *] \blacksquare \exists!_{\langle a,b \rangle \in A \times B} (O = a + b)$$

$$(1.1.4) \quad (v \neq O) \implies (\neg \exists!_{\langle a,b \rangle \in A \times B} (O = a + b)) \implies \perp \blacksquare v = O$$

$$(1.2) \quad (v \in A \cap B) \implies (v = O) \blacksquare A + B \subseteq \{O\}$$

$$(1.3) \quad (v = O) \implies \dots$$

$$(1.3.1) \quad (Subspace[A, V, +, *]) \wedge (Subspace[B, V, +, *]) \blacksquare (O \in A) \wedge (O \in B) \blacksquare v = O \in A \cup B$$

$$(1.4) \quad (v = O) \implies (v \in A \cap B) \blacksquare \{O\} \subseteq A \cap B$$

$$(1.5) \quad (A + B \subseteq \{O\}) \wedge (\{O\} \subseteq A \cap B) \blacksquare A \cap B = \{O\}$$

$$(2) \quad (DirSum[A \oplus B, A, B, V, +, *]) \implies (A \cap B = \{O\})$$

$$(3) \quad (A \cap B = \{O\}) \implies \dots$$

$$(3.1) \quad (O \in A) \wedge (O \in B) \wedge (O = O + O \in A + B) \blacksquare \exists_{\langle a,b \rangle \in A \times B} (O = a + b)$$

$$(3.2) \quad (((\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle) \in A \times B) \wedge (O = a_1 + b_1) \wedge (O = a_2 + b_2)) \implies \dots$$

$$(3.2.1) \quad (O = a_1 + b_1) \wedge (O = a_2 + b_2) \blacksquare (a_1 = -b_1) \wedge (a_2 = -b_2)$$

$$(3.2.2) \quad VectorSpace[B, +, *] \blacksquare -b_1, -b_2 \in B$$

$$(3.2.3) \quad (a_1 \in A) \wedge (a_1 = -b_1 \in B) \blacksquare a_1 \in A \cap B \blacksquare a_1 = O \blacksquare a_1 = b_1 = O$$

$$(3.2.4) \quad (a_2 \in A) \wedge (a_2 = -b_2 \in B) \blacksquare a_2 \in A \cap B \blacksquare a_2 = O \blacksquare a_2 = b_2 = O$$

$$(3.2.5) \quad \langle a_1, b_1 \rangle = \langle O, O \rangle = \langle a_2, b_2 \rangle$$

$$(3.3) \quad (((\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle) \in A \times B) \wedge (O = a_1 + b_1) \wedge (O = a_2 + b_2)) \implies (\langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle)$$

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

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

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

$$(4) \quad (A \cap B = \{O\}) \implies (DirSum[A \oplus B, A, B, V, +, *])$$

$$(5) \quad (DirSum[A \oplus B, A, B, V, +, *]) \iff (A \cap B = \{O\})$$

$$NullSpace[N, A, m, n] := (Matrix[A, m, n]) \wedge (N = \{x \in \mathbb{R}^n \mid A * x = O\})$$

$$RowSpace[R, A, m, n] := (Matrix[A, m, n]) \wedge (R = \{x^T * A \in \mathbb{R}^n \mid x \in \mathbb{R}^m\})$$

$$ColSpace[C, A, m, n] := (Matrix[A, m, n]) \wedge (C = \{A * x \in \mathbb{R}^m \mid x \in \mathbb{R}^n\})$$

$$NullSubspace := (NullSpace[N, A, m, n]) \implies (Subspace[N, \mathbb{R}^n, +, *])$$

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

$$RowSubspace := (RowSpace[R, A, m, n]) \implies (Subspace[R, \mathbb{R}^n, +, *])$$

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

$$ColSubspace := (ColSpace[C, A, m, n]) \implies (Subspace[C, \mathbb{R}^m, +, *])$$

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

### 3.5 Linear Combination, Linear Span, Linear Independence

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

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

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

(1)  $(S = \emptyset) \implies \dots$

(1.1)  $LinSpan[S', S, V, +, *] \blacksquare S' = \{O\}$

(1.2)  $Subspace[\{O\}, V, +, *] \blacksquare Subspace[S', V, +, *]$

(1.3)  $S = \emptyset \subseteq \{O\} = S' \blacksquare S \subseteq S'$

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

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

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

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

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

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

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

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

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

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

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

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

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

(3.6)  $((r \in \mathbb{R}) \wedge (u \in S')) \implies \dots$

(3.6.1)  $\exists_{K \in \mathbb{R}^n} (LinComb[u, S, K, V, +, *]) \blacksquare u = \sum_{i=1}^n (k_i * s_i)$

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

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

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

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

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

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

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

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

(3.9.2)  $\exists_{K \in \mathbb{R}^n} (LinComb[s_j, S, K, V, +, *]) \blacksquare s_j \in S'$

(3.10)  $(s_i \in S) \implies (s_i \in S') \blacksquare S \subseteq S'$

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

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

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

(6)  $\dots (Subspace[S', V, +, *]) \wedge (S \subseteq S')$

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

(1)  $(s' \in S') \implies \dots$

(1.1)  $\exists_{K \in \mathbb{R}^n} (LinComb[s', S, K, V, +, *]) \blacksquare s' = \sum_{i=1}^n (k_i * s_i)$

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

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

$$Spans[S, V, +, *] := LinSpan[V, S, V, +, *]$$

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

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

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

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

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

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

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

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

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

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

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

$$(3) \quad \text{LinInd}[\langle v \rangle, V, +, *]$$

$$\text{SubIndependent} := \forall_{V,A,B} \left( ((\text{VectorSpace}[V, +, *]) \wedge (A \subseteq B) \wedge (A \in V^n) \wedge (B \in V^m)) \implies \right. \\ \left. ((\text{LinInd}[B, V, +, *]) \implies (\text{LinInd}[A, V, +, *])) \right)$$

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

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

$$(1.2) \quad A \subseteq B \quad \blacksquare \quad \forall_{j \in \mathbb{N}_{1,n}} (a_j = b_j) \quad \blacksquare \quad \sum_{i=1}^n (k_i * a_i) = \sum_{j=1}^m (l_j * b_j)$$

$$(1.3) \quad \text{LinComb}[O, A, K, V, +, *] \quad \blacksquare \quad O = \sum_{i=1}^n (k_i * a_i) = \sum_{j=1}^m (l_j * b_j) \quad \blacksquare \quad \text{LinComb}[O, B, L, V, +, *]$$

$$(1.4) \quad (\text{LinInd}[B, V, +, *]) \wedge (\text{LinComb}[O, B, L, V, +, *]) \quad \blacksquare \quad L = \{0\}^m \quad \blacksquare \quad K = \{0\}^n$$

$$(2) \quad ((K \in \mathbb{R}^n) \wedge (\text{LinComb}[O, A, K, V, +, *])) \implies (K = \{0\}^n) \quad \blacksquare \quad \text{LinInd}[A, V, +, *]$$

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

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

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

$$(3) \quad A \subseteq B \quad \blacksquare \quad \forall_{j \in \mathbb{N}_{1,n}} (a_j = b_j) \quad \blacksquare \quad \sum_{i=1}^n (k_i * a_i) = \sum_{j=1}^m (l_j * b_j)$$

$$(4) \quad \text{LinComb}[O, A, K, V, +, *] \quad \blacksquare \quad \text{LinComb}[O, B, L, V, +, *]$$

$$(5) \quad K \neq \{0\}^n \quad \blacksquare \quad L \neq \{0\}^m$$

$$(6) \quad \exists_L ((\text{LinComb}[O, B, L, V, +, *]) \wedge (L \neq \{0\}^m)) \quad \blacksquare \quad \neg \text{LinInd}[B, V, +, *]$$

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

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

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

$$(3) \quad \dots \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^j (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j \quad \blacksquare \quad \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j$$

$$(4) \quad (\text{LinComb}[O, S, K, V, +, *]) \wedge (\sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j) \quad \blacksquare \quad O = \sum_{i=1}^n (k_i * s_i) = \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j$$

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

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

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

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

$$(2) \quad \forall_{u \in P} ((\exists_{K_1} (\text{LinComb}[u, S, K_1, V, +, *])) \implies (\exists_{K_2} (\text{LinComb}[u, S \setminus \{s_j\}, K_2, V, +, *]))) \quad \blacksquare \quad \text{LinSpan}[P, S \setminus \{s_j\}, V, +, *]$$

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

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

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

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

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

$$(3.2) \text{LinComb}[s_j, S \setminus \{s_j\}, K, V, +, *] \blacksquare \dots \blacksquare \sum_{i=1}^{j-1} (k_i * s_i) + k_j * s_j = \sum_{i=1}^{j-1} (k_i * s_i) + - \sum_{i=1}^{j-1} (k_i * s_i) = O \dots$$

$$(3.3) \dots \text{LinComb}[O, S, L, V, +, *]$$

$$(3.4) (\text{LinComb}[O, S, L, V, +, *]) \wedge (L \neq \{0\}^n) \blacksquare \exists_{L \in \mathbb{R}^n} ((\text{LinComb}[O, S, L, V, +, *]) \wedge (L \neq \{0\}^n)) \blacksquare (\neg \text{LinInd}[S, V, +, *])$$

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

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

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

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

$$(1) (\neg \text{LinInd}[W, V, +, *]) \implies \dots$$

$$(1.1) \exists_{j \in W} (\text{LinComb}[j, W \setminus \{j\}, +, *]) \blacksquare \neg \text{LinInd}[W, U, +, *]$$

$$(1.2) (\text{LinInd}[W, U, +, *]) \wedge (\neg \text{LinInd}[W, U, +, *]) \blacksquare \perp$$

$$(2) (\neg \text{LinInd}[W, V, +, *]) \implies \perp \blacksquare \text{LinInd}[W, V, +, *]$$

### 3.6 Bases and Dimensions

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

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

$$(1) (\text{Basis}[S, V, +, *]) \implies \dots$$

$$(1.1) (v \in V) \implies \dots$$

$$(1.1.1) \text{Basis}[S, V, +, *] \blacksquare \text{Spans}[V, S, +, *] \blacksquare \exists_{K \in \mathbb{R}^n} (\text{LinComb}[v, S, K, V, +, *])$$

$$(1.1.2) ((K_1, K_2 \in \mathbb{R}^n) \wedge (\text{LinComb}[v, S, K_1, V, +, *]) \wedge (\text{LinComb}[v, S, K_2, V, +, *])) \implies \dots$$

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

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

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

$$(1.1.2.4) (\text{LinInd}[S, V, +, *]) \wedge (\text{LinComb}[O, S, L, V, +, *]) \blacksquare L = \{0\}^n \blacksquare K_2 = K_1$$

$$(1.1.3) ((K_1, K_2 \in \mathbb{R}^n) \wedge (\text{LinComb}[v, S, K_1, V, +, *]) \wedge (\text{LinComb}[v, S, K_2, V, +, *])) \implies (K_1 = K_2)$$

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

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

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

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

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

$$(3.1) \forall_{v \in V} \exists!_{K \in \mathbb{R}^n} (\text{LinComb}[v, S, K, V, +, *]) \blacksquare \forall_{v \in V} \exists_{K \in \mathbb{R}^n} (\text{LinComb}[v, S, K, V, +, *]) \blacksquare \text{Spans}[S, V, +, *]$$

$$(3.2) O \in V \blacksquare \exists!_{K \in \mathbb{R}^n} (\text{LinComb}[O, S, K, V, +, *])$$

$$(3.3) (K \neq \{0\}^n) \implies (\neg \exists!_{K \in \mathbb{R}^n} (\text{LinComb}[O, S, K, V, +, *])) \implies \perp \blacksquare K = \{0\}^n$$

$$(3.4) (\exists!_{K \in \mathbb{R}^n} (\text{LinComb}[O, S, K, V, +, *])) \wedge (K = \{0\}^n) \blacksquare \text{LinInd}[S, V, +, *]$$

$$(3.5) (\text{Spans}[S, V, +, *]) \wedge (\text{LinInd}[S, V, +, *]) \blacksquare \text{Basis}[S, V, +, *]$$

$$(4) (\forall_{v \in V} \exists!_{K \in \mathbb{R}^n} (\text{LinComb}[v, S, K, V, +, *])) \implies (\text{Basis}[S, V, +, *])$$

$$\text{SpanReduceBasis} := \forall_{S,V} ((\text{Spans}[S, V, +, *]) \implies (\exists_B ((B \subseteq S) \wedge (\text{Basis}[B, V, +, *]))))$$

$$(1) \text{LinDepPropCorollary} \blacksquare \exists_B ((B \subseteq S) \wedge (\text{LinInd}[B, V, +, *]) \wedge (\text{Spans}[B, V, +, *])) \blacksquare \exists_B ((B \subseteq S) \wedge (\text{Basis}[B, V, +, *]))$$

$$(2) \text{TODO - formalize removing latter entries first}$$

$$FinDimBasis := \forall_V((FinDim[V, +, *]) \implies (\exists_B(Basis[B, V, +, *])))$$

$$(1) \quad FinDim[V, +, *] \quad \blacksquare \quad \exists_{S \in V^n}(Spans[S, V, +, *])$$

$$(2) \quad (SpanReduceBasis) \wedge (Spans[S, V, +, *]) \quad \blacksquare \quad \exists_B(Basis[B, V, +, *])$$

$$LinIndExpandBasis := \forall_{L,V}((LinInd[L, V, +, *]) \implies (\exists_B((L \subseteq B) \wedge (Basis[B, V, +, *])))$$

$$(1) \quad FinDimBasis \quad \blacksquare \quad \exists_C(Basis[C, V, +, *])$$

$$(2) \quad S := L \cup C$$

$$(3) \quad Basis[C, V, +, *] \quad \blacksquare \quad Spans[C, V, +, *] \quad \blacksquare \quad Spans[S, V, +, *]$$

$$(4) \quad SpanReduceBasis \quad \blacksquare \quad (\exists_B((B \subseteq S) \wedge (Basis[B, V, +, *]))) \wedge (L \subseteq B)$$

$$SpanLinIndLength := \forall_{S,T,V}(((Span[S, V, +, *]) \wedge (LinInd[T, V, +, *])) \implies (|T| \leq |S|))$$

$$(1) \quad ((Span[S, V, +, *]) \wedge (|T| > |S|)) \implies \dots$$

$$(1.1) \quad Span[S, V, +, *] \quad \blacksquare \quad \forall_{i \in \mathbb{N}_{1,|H|}} \exists_{K_i \in \mathbb{R}^{|S|}}(LinComb[t_i, S, K_i V, +, *])$$

$$(1.2) \quad |H| > |S| \quad \blacksquare \quad \exists_{L \in \mathbb{R}^{|H|-1}}(LinComb[t_{|H|}, T \setminus \{t_{|H|}\}, L, V, +, *])$$

$$(1.3) \quad L = -1 * K \quad \blacksquare \quad (\sum(K + L) = 0) \wedge (K + L \neq \{0\}^{|T|}) \quad \blacksquare \quad \neg LinInd[T, V, +, *]$$

$$(1.4) \quad \text{TODO - tidy up}$$

$$(2) \quad ((Span[S, V, +, *]) \wedge (|T| > |S|)) \implies (\neg LinInd[T, V, +, *]) \quad \blacksquare \quad ((Span[S, V, +, *]) \wedge (LinInd[T, V, +, *])) \implies (|T| \leq |S|)$$

$$BasisLength := \forall_{S,T,V}(((Basis[S, V, +, *]) \wedge (Basis[T, V, +, *])) \implies (|T| = |S|))$$

$$(1) \quad (Span[T, V, +, *]) \wedge (LinInd[S, V, +, *]) \quad \blacksquare \quad |S| \leq |T|$$

$$(2) \quad (Span[S, V, +, *]) \wedge (LinInd[T, V, +, *]) \quad \blacksquare \quad |T| \leq |S|$$

$$(3) \quad (|S| \leq |T|) \wedge (|T| \leq |S|) \quad \blacksquare \quad |T| = |S|$$

$$Dim[d, V, +, *] := ((V = \{O\}) \implies (d = 0)) \wedge ((V \neq \{O\}) \implies ((\exists_B(Basis[B, V, +, *])) \wedge (d = |B|)))$$

$$LinIndLengthDim := \forall_{U,V}(((LinInd[U, V, +, *]) \wedge (Dim[|U|, V, +, *])) \implies (Basis[U, V, +, *]))$$

$$(1) \quad (LinIndExpandBasis) \wedge (LinInd[U, V, +, *]) \quad \blacksquare \quad \exists_B((U \subseteq B) \wedge (Basis[B, V, +, *]))$$

$$(2) \quad (BasisLength) \wedge (Dim[|U|, V, +, *]) \wedge (Basis[B, V, +, *]) \quad \blacksquare \quad |B| = |U| \quad \blacksquare \quad B = U \quad \blacksquare \quad Basis[U, V, +, *]$$

$$SpanLengthDim := \forall_{U,V}(((Spans[U, V, +, *]) \wedge (Dim[|U|, V, +, *])) \implies (Basis[U, V, +, *]))$$

$$(1) \quad (SpanReduceBasis) \wedge (Spans[U, V, +, *]) \quad \blacksquare \quad \exists_B((B \subseteq U) \wedge (Basis[B, V, +, *]))$$

$$(2) \quad (BasisLength) \wedge (Dim[|U|, V, +, *]) \wedge (Basis[B, V, +, *]) \quad \blacksquare \quad |B| = |U| \quad \blacksquare \quad B = U \quad \blacksquare \quad Basis[U, V, +, *]$$

$$LinDepLengthDim := \forall_{U,V}(((U \subseteq V) \wedge (|U| > Dim[V])) \implies (\neg LinInd[U, V, +, *]))$$

$$(1) \quad \text{Contrapositive of } BasisLinearIndCard$$

$$(2) \quad \text{TODO - cleanup}$$

$$NonSpanLengthDim := \forall_{U,V}(((U \subseteq V) \wedge (|U| < Dim[V])) \implies (\neg Spans[U, V, +, *]))$$

$$(1) \quad \text{Suppose } Spans[U, V, +, *], B = SpanReduceBasis[U] \text{ to form a basis, } (|B| \leq |U| < Dim[V]) \wedge |B| = Dim[V] \quad \blacksquare \quad \perp$$

$$(2) \quad \neg Spans[U, V, +, *]$$

$$(3) \quad \text{TODO - cleanup}$$

## 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

---

$$\text{RankNullity} := \forall_A((\text{Matrix}[A, m, n]) \implies (\text{Rank}[A] + \text{Nullity}[A] = n))$$

(1) TODO

---

$$\text{RankInv} := \forall_A((\text{Matrix}[A, m, n]) \implies ((\text{Rank}[A] = n) \iff (\text{Inv}[A])))$$

(1) TODO

---

$$\text{RankNonTrivialSol} := (\exists_X((A * X = O) \wedge (X \neq O))) \iff (\text{Rank}[A] < n)$$

(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

---

$$\text{SquareTheorems}_8 := \forall_{A \in \mathcal{M}} \left( \begin{array}{l} (\text{Invertible}[A]) \iff \\ (\text{RowEquiv}[A, I_n]) \iff \\ (\forall_X((X = O) \iff (\text{Sol}[X, A, O]))) \iff \\ (\forall_{B \in \mathcal{M}} \exists!_{X \in \mathcal{M}}(\text{Sol}[X, A, B])) \iff \\ (\text{Rank}[A] = n) \iff \\ (\text{Nullity}[A] = 0) \iff \\ (\text{The rows form a linearly independent set of vectors (to get full rank)}) \iff \\ (\text{The columns form a linearly independent set of vectors (to get full rank)}) \iff \end{array} \right)$$

### 3.8 Linear Transformations

$$\text{LinTrans}[L, V, +_v, *_v, W, +_w, *_w] := \left( \begin{array}{l} (\text{Function}[f, V, W]) \wedge (\text{VectorSpace}[V, +_v, *_v]) \wedge (\text{VectorSpace}[W, +_w, *_w]) \wedge \\ (\forall_{\alpha, \beta \in V} (L(\alpha +_v \beta) = L(\alpha) +_w L(\beta))) \quad \wedge \quad (\forall_{r \in \mathbb{R}} \forall_{\alpha \in V} (L(r *_v \alpha) = r *_w L(\alpha))) \end{array} \right)$$

$$\text{LinOp}[L, V, +_v, *_v] := \text{LinTrans}[L, V, +_v, *_v, V, +_v, *_v]$$

$$\mathcal{L}[V, W] := \{L \mid \text{LinTrans}[L, V, +_v, *_v, W, +_w, *_w]\}$$

$$\text{ZeroMapsToZero} := \forall_{L, V, W}((\text{LinTrans}[L, V, +_v, *_v, W, +_w, *_w]) \implies (L(O_v) = O_w))$$

(1)  $L(O_v) = L(O_v +_v O_v) = L(O_v) +_w L(O_v)$

(2)  $O_w = L(O_v) - L(O_v) = L(O_v)$

---

$$\text{SplitAddInv} := \forall_{L, V, W}((\text{LinTrans}[L, V, +_v, *_v, W, +_w, *_w]) \implies (\forall_{\alpha, \beta \in V} (L(\alpha -_v \beta) = L(\alpha) -_w L(\beta))))$$

(1)  $L(\alpha - \beta) = L(\alpha + (-\beta)) = L(\alpha) + L(-\beta) = L(\alpha) + (-1) * L(\beta) = L(\alpha) - L(\beta)$

---

$$\text{UniqBasisLT} := \forall_{V, W} \left( \begin{array}{l} ((\text{VectorSpace}[V, +_v, *_v]) \wedge (\text{VectorSpace}[W, +_w, *_w]) \wedge (\text{Basis}[A, V, +_v, *_v]) \wedge (\text{Basis}[B, W, +_w, *_w])) \implies \\ (\exists!_T((\text{LinTrans}[T, V, +_v, *_v, W, +_w, *_w]) \wedge (\forall_{i \in \mathbb{N}_{1,n}} (T(a_i) = b_i)))) \end{array} \right)$$

(1)  $T(\sum_{i=1}^n (k_i * a_i)) := \sum_{i=1}^n (k_i * b_i)$

(2)  $(i \in \mathbb{N}_{1,n}) \implies \dots$

---

$$(2.1) \quad L := \left\langle \left\{ \begin{array}{ll} 1 & j = i \\ 0 & j \neq i \end{array} \right\} \mid j \in \mathbb{N}_{1,n} \right\rangle \quad \blacksquare \quad L \in \mathbb{R}^n$$

$$(2.2) \quad T(a_i) = T(\sum_{i=1}^n (l_i * a_i)) = \sum_{i=1}^n (l_i * b_i) = b_i \quad \blacksquare \quad T(a_i) = b_i$$

(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)  $(\alpha, \beta \in V) \implies \dots$

$$(6.1) \quad (\exists_{K_\alpha} (\text{LinComb}[\alpha, A, K_\alpha, V, +_v, *_v]) \wedge (\exists_{K_\beta} (\text{LinComb}[\beta, A, K_\beta, V, +_v, *_v]))) \quad \blacksquare \quad (\alpha = \sum_{i=1}^n (k_{\alpha i} * a_i)) \wedge (\beta = \sum_{i=1}^n (k_{\beta i} * a_i))$$

$$(6.2) \quad T(\alpha + \beta) = T(\sum_{i=1}^n (k_{\alpha i} * a_i) + \sum_{i=1}^n (k_{\beta i} * a_i)) = T(\sum_{i=1}^n ((k_{\alpha i} + k_{\beta i}) * a_i)) = \sum_{i=1}^n ((k_{\alpha i} + k_{\beta i}) * b_i) = \dots$$

(6.3)	$\dots \sum_{i=1}^n (k_{\alpha_i} * b_i) + \sum_{i=1}^n (k_{\beta_i} * b_i) = T(\sum_{i=1}^n (k_{\alpha_i} * a_i)) + T(\sum_{i=1}^n (k_{\beta_i} * a_i)) = T(\alpha) + T(\beta)$
(7)	$(\alpha, \beta \in V) \implies (L(\alpha +_v \beta) = L(\alpha) +_w L(\beta)) \blacksquare \forall_{\alpha, \beta \in V} (L(\alpha +_v \beta) = L(\alpha) +_w L(\beta))$
(8)	$((r \in \mathbb{R}) \wedge (\alpha \in V)) \implies \dots$
(8.1)	$\exists_K (LinComb[\alpha, A, K, V, +_v, *_v]) \blacksquare \alpha = \sum_{i=1}^n (k_i * a_i)$
(8.2)	$L(r *_v \alpha) = L(r *_v \sum_{i=1}^n (k_i *_v a_i)) = L(\sum_{i=1}^n ((rk_i) *_v a_i)) = \dots$
(8.3)	$\dots \sum_{i=1}^n ((rk_i) *_w b_i) = r *_w \sum_{i=1}^n (k_i *_w b_i) = r *_w L(\sum_{i=1}^n (k_i *_v a_i)) = r *_w L(\alpha)$
(9)	$((r \in \mathbb{R}) \wedge (\alpha \in V)) \implies (L(r *_v \alpha) = r *_w L(\alpha)) \blacksquare \forall_{r \in \mathbb{R}} \forall_{\alpha \in V} (L(r *_v \alpha) = r *_w L(\alpha))$
(10)	$(\forall_{i \in \mathbb{N}_{1,n}} (T(a_i) = b_i)) \wedge (Function[T, V, W]) \wedge (\forall_{\alpha, \beta \in V} (L(\alpha +_v \beta) = L(\alpha) +_w L(\beta))) \wedge (\forall_{r \in \mathbb{R}} \forall_{\alpha \in V} (L(r *_v \alpha) = r *_w L(\alpha))) \wedge \dots$
(11)	$\dots (VectorSpace[V, +_v, *_v]) \wedge (VectorSpace[W, +_w, *_w]) \blacksquare (\forall_{i \in \mathbb{N}_{1,n}} (T(a_i) = b_i)) \wedge (LinTrans[T, V, +_v, *_v, W, +_w, *_w])$
(12)	$(\forall_{i \in \mathbb{N}_{1,n}} (T_2(a_i) = b_i)) \wedge (LinTrans[T_2, V, +_v, *_v, W, +_w, *_w]) \implies \dots$
(12.1)	$\forall_{i \in \mathbb{N}_{1,n}} (T_2(a_i) = b_i) \blacksquare \forall_{i \in \mathbb{N}_{1,n}} (T_2(c_i * a_i) = c_i * b_i) \blacksquare T_2(\sum_{i=1}^n (c_i * a_i)) = \sum_{i=1}^n (c_i * b_i) \blacksquare T_2 = T$
(13)	$(\forall_{i \in \mathbb{N}_{1,n}} (T_2(a_i) = b_i)) \wedge (LinTrans[T_2, V, +_v, *_v, W, +_w, *_w]) \implies (T_2 = T)$

$+_{\mathcal{L}}[S + T, S, T] := (S + T)(v) = S(v) + T(v)$   
 $*_{\mathcal{L}}[r * T, r, T] := (r * T)(v) = r * (T(v))$   
 $LTVectorSpace := \forall_{V, W} (VectorSpace[\mathcal{L}[V, W], +_{\mathcal{L}}, *__{\mathcal{L}}])$

(1) TODO

$*_{\mathcal{L}}[S * T, S, T] := (S * T)(v) = S(T(v))$   
 $LTProdProperties := (associativity) \wedge (identity) \wedge (distributive)$

(1) TODO

$Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w] := (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (ker_L = \{\alpha \in V \mid L(\alpha) = O_w\})$

$KerSubspace := \forall_{L, V, W} ((Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w]) \implies (Subspace[ker_L, V, +_v, *_v]))$

(1)  $ZeroMapsToZero \blacksquare L(O_v) = O_w \blacksquare O_v \in ker_L \blacksquare \emptyset \neq ker_L \blacksquare \emptyset \neq ker_L \subseteq V$

(2)  $(\alpha, \beta \in ker_L) \implies \dots$

(2.1)  $(L(\alpha) = O_w) \wedge (L(\beta) = O_w)$

(2.2)  $L(\alpha + \beta) = L(\alpha) + L(\beta) = O_w + O_w = O_w \blacksquare L(\alpha + \beta) \in ker_L$

(3)  $(\alpha, \beta \in ker_L) \implies (\alpha + \beta \in ker_L) \blacksquare \forall_{\alpha, \beta \in ker_L} (\alpha + \beta \in ker_L)$

(4)  $((r \in \mathbb{R}) \wedge (\alpha \in ker_L)) \implies \dots$

(4.1)  $L(\alpha) = O_w \blacksquare L(r * \alpha) = r * L(\alpha) = r * O_w = O_w \blacksquare r * \alpha \in ker_L$

(5)  $((r \in \mathbb{R}) \wedge (\alpha \in ker_L)) \implies (r * \alpha \in ker_L) \blacksquare \forall_{r \in \mathbb{R}} \forall_{\alpha \in ker_L} (r * \alpha \in ker_L)$

(6)  $(SubspaceEquiv) \wedge (\emptyset \neq ker_L \subseteq V) \wedge (\forall_{\alpha, \beta \in ker_L} (\alpha + \beta \in ker_L)) \wedge (\forall_{r \in \mathbb{R}} \forall_{\alpha \in ker_L} (r * \alpha \in ker_L)) \blacksquare Subspace[ker_L, V, +_v, *_v]$

$Rng[rng_L, L, V, +_v, *_v, W, +_w, *_w] := (LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (rng_L = \{\beta \in W \mid \exists_{\alpha \in V} (\beta = L(\alpha))\})$

$RangeSubspace := \forall_{L, V, W} ((Ran[rng_L, L, V, +_v, *_v, W, +_w, *_w]) \implies (Subspace[rng_L, W, +_w, *_w]))$

(1)  $ZeroMapsToZero \blacksquare O_w = L(O_v) \blacksquare \exists_{\alpha \in V} (O_w = L(\alpha)) \blacksquare O_w \in rng_L \blacksquare \emptyset \neq rng_L \blacksquare \emptyset \neq rng_L \subseteq W$

(2)  $(\alpha, \beta \in rng_L) \implies \dots$

(2.1)  $(\exists_{u \in V} (\alpha = L(u))) \wedge (\exists_{v \in V} (\beta = L(v)))$

(2.2)  $\alpha + \beta = L(u) + L(v) = L(u + v) \blacksquare \exists_{w \in V} (\alpha + \beta = L(w)) \blacksquare \alpha + \beta \in rng_L$

(3)  $(\alpha, \beta \in rng_L) \implies (\alpha + \beta \in rng_L) \blacksquare \forall_{\alpha, \beta \in rng_L} (\alpha + \beta \in rng_L)$

(4)  $((r \in \mathbb{R}) \wedge (\alpha \in rng_L)) \implies \dots$

(4.1)  $\exists_{v \in V} (\alpha = L(v)) \blacksquare L(r * v) = r * L(v) = r * \alpha \blacksquare \exists_{w \in V} (r * \alpha = L(w)) \blacksquare r * \alpha \in rng_L$

(5)  $((r \in \mathbb{R}) \wedge (\alpha \in rng_L)) \implies (r * \alpha \in rng_L) \blacksquare \forall_{r \in \mathbb{R}} \forall_{\alpha \in rng_L} (r * \alpha \in rng_L)$

(6)  $(SubspaceEquiv) \wedge (\emptyset \neq rng_L \subseteq W) \wedge (\forall_{\alpha, \beta \in rng_L} (\alpha + \beta \in rng_L)) \wedge (\forall_{r \in \mathbb{R}} \forall_{\alpha \in rng_L} (r * \alpha \in rng_L)) \blacksquare Subspace[rng_L, W, +_w, *_w]$

$$KerInj := \forall_{L,V,W} ((Ker[ker_L, L, V, +_v, *_v, W, +_w, *_w]) \implies ((Inj[L, V, W]) \iff (ker_L = \{O_v\})))$$

$$(1) \quad (Inj[L, V, W]) \implies \dots$$

$$(1.1) \quad ZeroMapsToZero \quad \blacksquare \quad L(O_v) = O_w$$

$$(1.2) \quad O_v \in ker_L \quad \blacksquare \quad \{O_v\} \subseteq ker_L$$

$$(1.3) \quad (v \in ker_L) \implies \dots$$

$$(1.3.1) \quad L(v) = O_w$$

$$(1.3.2) \quad (Inj[L, V, W]) \wedge (L(O_v) = O_w) \quad \blacksquare \quad O_v = v$$

$$(1.4) \quad (v \in ker_L) \implies (v = O_v) \quad \blacksquare \quad ker_L \subseteq \{O_v\}$$

$$(1.5) \quad (\{O_v\} \subseteq ker_L) \wedge (ker_L \subseteq \{O_v\}) \quad \blacksquare \quad ker_L = \{O_v\}$$

$$(2) \quad (Inj[L, V, W]) \implies (ker_L = \{O_v\})$$

$$(3) \quad (ker_L = \{O_v\}) \implies \dots$$

$$(3.1) \quad ((u, v \in V) \wedge (L(u) = L(v))) \implies \dots$$

$$(3.1.1) \quad O_w = L(u) - L(v) = L(u - v) \quad \blacksquare \quad u - v \in ker_L$$

$$(3.1.2) \quad ker_L = \{O_v\} \quad \blacksquare \quad u - v = O_v \quad \blacksquare \quad u = v$$

$$(3.2) \quad ((u, v \in V) \wedge (L(u) = L(v))) \implies (u = v) \quad \blacksquare \quad \forall_{u,v \in V} ((L(u) = L(v)) \implies (u = v)) \quad \blacksquare \quad Inj[L, V, W]$$

$$(4) \quad (ker_L = \{O_v\}) \implies (Inj[L, V, W])$$

$$(5) \quad (Inj[L, V, W]) \iff (ker_L = \{O_v\})$$

$$RngSurj := \forall_{L,V,W} ((Ran[rng_L, L, V, +_v, *_v, W, +_w, *_w]) \implies ((Surj[L, V, W]) \iff (rng_L = W)))$$

$$(1) \quad (SurjEquiv) \wedge (rng(L) = rng_L) \quad \blacksquare \quad (Surj[L, V, W]) \iff (rng_L = W)$$

$$RankNullityLT := \forall_{L,V,W} ((LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \implies (Dim[V] = Dim[ker_L] + Dim[rng_L]))$$

$$(1) \quad KerSubspace \quad \blacksquare \quad (\exists_U (Basis[U, ker_L, +_v, *_v])) \wedge (Dim[ker_L] = |U|)$$

$$(2) \quad (LinIndSuperspace) \wedge (LinInd[U, ker_L, +_v, *_v]) \quad \blacksquare \quad LinInd[U, V, +_v, *_v]$$

$$(3) \quad (LinIndExpandBasis) \wedge (LinInd[U, V, +_v, *_v]) \quad \blacksquare \quad (\exists_B ((U \subseteq B) \wedge (Basis[B, V, +_v, *_v]))) \wedge (Dim[V] = |B|)$$

$$(4) \quad U \subseteq B \quad \blacksquare \quad \exists_T (B = U \cup T)$$

$$(5) \quad (w \in rng_L) \implies \dots$$

$$(5.1) \quad \exists_{v \in V} (w = L(v))$$

$$(5.2) \quad (Basis[B, V, +_v, *_v]) \wedge (B = U \cup T) \quad \blacksquare \quad \exists_{K \in \mathbb{R}^{|B|}} (v = \sum_{i=1}^{|B|} (k_i * b_i) = \sum_{i=1}^{|U|} (k_i * u_i) + \sum_{i=1}^{|T|} (k_{|U|+i} * t_i))$$

$$(5.3) \quad w = L(v) = L(\sum_{i=1}^{|U|} (k_i * u_i) + \sum_{i=1}^{|T|} (k_{|U|+i} * t_i)) = L(\sum_{i=1}^{|U|} (k_i * u_i)) + L(\sum_{i=1}^{|T|} (k_{|U|+i} * t_i)) = \dots$$

$$(5.4) \quad O + L(\sum_{i=1}^{|T|} (k_{|U|+i} * t_i)) = \sum_{i=1}^{|T|} (L(k_{|U|+i} * t_i)) = \sum_{i=1}^{|T|} (k_{|U|+i} * L(t_i)) \quad \blacksquare \quad \exists_K (LinComb[w, L(T), K, W, +, *])$$

$$(6) \quad (w \in rng_L) \implies (\exists_L (LinComb[w, L(T), L, W, +, *])) \quad \blacksquare \quad Spans[L(T), rng_L, W, +, *]$$

$$(7) \quad ((K \in \mathbb{R}^n) \wedge (LinComb[O_w, L(T), K, W, +_w, *_w])) \implies \dots$$

$$(7.1) \quad O_w = \sum_{i=1}^n (k_i * L(t_i)) = L(\sum_{i=1}^n (k_i * t_i)) \quad \blacksquare \quad \sum_{i=1}^n (k_i * t_i) \in ker_L$$

$$(7.2) \quad (Basis[U, ker_L, +_v, *_v]) \wedge (\sum_{i=1}^n (k_i * t_i) \in ker_L) \quad \blacksquare \quad \exists_{D \in \mathbb{R}^m} (\sum_{i=1}^n (k_i * t_i) = \sum_{i=1}^m (d_i * u_i))$$

$$(7.3) \quad Basis[B] \quad \blacksquare \quad LinInd[B] \quad \blacksquare \quad LinInd[U \cup T] \quad \blacksquare \quad \forall_{s_j \in U \cup T} \forall_{K \in \mathbb{R}^{n-1}} (\neg LinComb[s_j, U \cup T \setminus \{s_j\}, K, V, +, *])$$

$$(7.4) \quad (\sum_{i=1}^n (k_i * t_i) = \sum_{i=1}^m (d_i * u_i)) \wedge (\forall_{s_j \in U \cup T} \forall_{K \in \mathbb{R}^{n-1}} (\neg LinComb[s_j, U \cup T \setminus \{s_j\}, K, V, +, *])) \quad \blacksquare \quad (D = \{O\}) \wedge (K = \{O\})$$

$$(8) \quad ((K \in \mathbb{R}^n) \wedge (LinComb[O_w, L(T), K, W, +_w, *_w])) \implies (K = \{O\}) \quad \blacksquare \quad LinInd[L(T), W, +_w, *_w]$$

$$(9) \quad (SubIndependent) \wedge (LinInd[L(T), W, +_w, *_w]) \quad \blacksquare \quad LinInd[L(T), rng_L, +_w, *_w]$$

$$(10) \quad (Spans[L(T), rng_L, W, +, *]) \wedge (LinInd[L(T), rng_L, +_w, *_w]) \quad \blacksquare \quad Basis[L(T), rng_L, +_w, *_w] \quad \blacksquare \quad Dim[rng_L] = |L(T)| = |T|$$

$$(11) \quad B = U \cup T \quad \blacksquare \quad |B| = |U| + |T| \quad \blacksquare \quad Dim[V] = Dim[ker_L] + Dim[rng_L]$$

$$InjSurjEqualDim := \forall_{T,V,W} \left( \begin{array}{l} ((LinTrans[T, V, +_v, *_v, W, +_w, *_w]) \wedge (Dim[V] = Dim[W]) \wedge (Inj[T, V, W])) \implies \\ (Surj[T, V, W]) \end{array} \right)$$

$$(1) \quad (KerInj) \wedge (Inj[T, V, W]) \quad \blacksquare \quad ker_T = \{O\} \quad \blacksquare \quad Dim[ker_T] = 0$$

$$(2) \quad (RankNullityLT) \wedge (Dim[ker_T] = 0) \quad \blacksquare \quad Dim[V] = Dim[ker_T] + Dim[rng_T] = Dim[rng_T] \quad \blacksquare \quad Dim[V] = Dim[rng_T]$$

$$(3) \quad (Dim[V] = Dim[W]) \wedge (Dim[V] = Dim[rng_T]) \quad \blacksquare \quad Dim[W] = Dim[rng_T]$$

$$(4) \quad RangeSubspace \quad \blacksquare \quad Subspace[rng_T, W, +_w, *_w]$$

$$(1.6) \quad (Inj[L, V, W]) \wedge (Surj[L, V, W])$$

(2)	$(LTInvertible[L, V, +_v, *_v, W, +_w, *_w]) \implies ((Inj[L, V, W]) \wedge (Surj[L, V, W]))$
(3)	$((Inj[L, V, W]) \wedge (Surj[L, V, W])) \implies \dots$
(3.1)	$(Inj[L, V, W]) \wedge (Surj[L, V, W]) \blacksquare \forall_{w \in W} \exists!_{v \in V} (w = L(v))$
(3.2)	$S := \{(w, v) \in W \times V \mid w = L(v)\}$
(3.3)	$(\forall_{w \in W} \exists!_{v \in V} (w = L(v))) \wedge (S = \{(w, v) \in W \times V \mid w = L(v)\}) \blacksquare Function[S, W, V]$
(3.4)	$(\forall_{v \in V} (S(L(v)) = v)) \wedge (\forall_{w \in W} (L(S(w)) = w))$
(3.5)	$(w_1, w_2 \implies W) \implies \dots$
(3.5.1)	$(LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (\forall_{w \in W} (L(S(w)) = w)) \blacksquare L(S(w_1) + S(w_2)) = L(S(w_1)) + L(S(w_2)) = w_1 + w_2$
(3.5.2)	$(\forall_{w \in W} (L(S(w)) = w)) \wedge (w_1 + w_2 \in W) \blacksquare L(S(w_1 + w_2)) = w_1 + w_2$
(3.5.3)	$L(S(w_1) + S(w_2)) = w_1 + w_2 = L(S(w_1 + w_2)) \blacksquare L(S(w_1) + S(w_2)) = L(S(w_1 + w_2))$
(3.5.4)	$(Inj[L, V, W]) \wedge (L(S(w_1) + S(w_2)) = L(S(w_1 + w_2))) \blacksquare S(w_1) + S(w_2) = S(w_1 + w_2)$
(3.6)	$(w_1, w_2 \implies W) \implies (S(w_1 + w_2) = S(w_1) + S(w_2)) \blacksquare \forall_{w_1, w_2 \in W} (S(w_1 + w_2) = S(w_1) + S(w_2))$
(3.7)	$((r \in \mathbb{R}) \wedge (w \in W)) \implies \dots$
(3.7.1)	$(LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (\forall_{w \in W} (L(S(w)) = w)) \blacksquare L(r * S(w)) = r * L(S(w)) = r * w$
(3.7.2)	$(\forall_{w \in W} (L(S(w)) = w)) \wedge (r * w \in W) \blacksquare L(S(r * w)) = r * w$
(3.7.3)	$L(r * S(w)) = r * w = L(S(r * w)) \blacksquare L(r * S(w)) = L(S(r * w))$
(3.7.4)	$(Inj[L, V, W]) \wedge (L(r * S(w)) = L(S(r * w))) \blacksquare r * S(w) = S(r * w)$
(3.8)	$((r \in \mathbb{R}) \wedge (w \in W)) \implies (r * S(w) = S(r * w)) \blacksquare \forall_{r \in \mathbb{R}} \forall_{w \in W} (S(r * w) = r * S(w))$
(3.9)	$(Function[S, W, V]) \wedge (\forall_{w_1, w_2 \in W} (S(w_1 + w_2) = S(w_1) + S(w_2))) \wedge (\forall_{r \in \mathbb{R}} \forall_{w \in W} (S(r * w) = r * S(w)))$
(3.10)	$LinTrans[S, W, +_w, *_w, V, +_v, *_v]$
(3.11)	$\forall_{v \in V} ((S(L(v)) = v)) \blacksquare S \circ L = 1_v$
(3.12)	$\forall_{w \in W} (L(S(w)) = w) \blacksquare L \circ S = 1_w$
(3.13)	$(LinTrans[S, W, +_w, *_w, V, +_v, *_v]) \wedge (S \circ L = 1_v) \wedge (L \circ S = 1_w) \blacksquare LTInv[S, L, V, +_v, *_v, W, +_w, *_w]$
(3.14)	$\exists_{L^{-1}} (LTInv[L^{-1}, L, V, +_v, *_v, W, +_w, *_w]) \blacksquare LTInvertible[L, V, +_v, *_v, W, +_w, *_w]$
(4)	$((Inj[L, V, W]) \wedge (Surj[L, V, W])) \implies (LTInvertible[L, V, +_v, *_v, W, +_w, *_w])$
(5)	$(LTInvertible[L, V, +_v, *_v, W, +_w, *_w]) \iff ((Inj[L, V, W]) \wedge (Surj[L, V, W]))$

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

$CoordVec[[\alpha]_S, \alpha, S, V, +, *] := (Basis[S, V, +, *]) \wedge (S * [\alpha]_S = \alpha \in V)$

$LTMatrix := \forall_{L, V, W} \left( \begin{array}{l} ((LinTrans[L, V, +_v, *_v, W, +_w, *_w]) \wedge (Basis[A, V, +_v, *_v]) \wedge (Basis[B, W, +_w, *_w])) \implies \\ (\forall_{v \in V} (CoordVec[[L(v)]_B, L(v), B, W, +_w, *_w] = \langle [L(a_i)]_B \mid a_i \in A \rangle * CoordVec[[v]_A, v, A, V, +_v, *_v])) \end{array} \right)$

(1)	$Basis[A, V, +_v, *_v] \blacksquare \exists_{K \in \mathbb{R}^n} (v = \sum_{i=1}^n (k_i * a_i)) \blacksquare K^T = CoordVec[[v]_A, v, A, V, +, *]$
(2)	$[L(v)]_B = [L(\sum_{i=1}^n (k_i * a_i))]_B = [\sum_{i=1}^n (L(k_i * a_i))]_B = \sum_{i=1}^n ([L(k_i * a_i)]_B) = \sum_{i=1}^n ([k_i * L(a_i)]_B) = \sum_{i=1}^n (k_i * [L(a_i)]_B) = \dots$
(3)	$\dots \langle [L(a)]_B \mid a \in A \rangle * K^T = \langle [L(a)]_B \mid a \in A \rangle * [v]_A \blacksquare [L(v)]_B = \langle [L(a)]_B \mid a \in A \rangle * [v]_A$

Note: Shorthand is to RREF the augmented matrix [Columns of B | Columns of A] into [I | M], thus M is the transition matrix

$TransitionMatrix := \forall_{L, V} \left( \begin{array}{l} ((Basis[A, V, +, *]) \wedge (Basis[B, V, +, *])) \implies \\ (\forall_{v \in V} (CoordVec[[v]_B, v, B, W, +_w, *_w] = \langle [a]_B \mid a \in A \rangle * CoordVec[[v]_A, v, A, V, +_v, *_v])) \end{array} \right)$

(1)	$(LTMatrix) \wedge (LinTrans[I, V, +, *, V, +, *]) \blacksquare [I(v)]_B = \langle [I(a)]_B \mid a \in A \rangle * [v]_A \blacksquare [v]_B = \langle [a]_B \mid a \in A \rangle * [v]_A$
-----	---

$LTOverTransition := ((([L(a)]_T = A * [a]_S) \wedge (P * [a]_{S'} = [a]_S) \wedge (Q * [L(a)]_{T'} = [L(a)]_T)) \implies ([L(a)]_{T'} = (Q^{-1} * A * P) * [a]_{S'}))$

(1)	$[L(a)]_{T'} = Q^{-1} * [L(a)]_T = Q^{-1} * A * [a]_S = Q^{-1} * A * P * [a]_{S'} \blacksquare [L(a)]_{T'} = (Q^{-1} * A * P) * [a]_{S'}$
-----	---

$LOOverTransition := ((([L(a)]_S = A * [a]_S) \wedge (P * [a]_{S'} = [a]_S)) \implies ([L(a)]_{S'} = (P^{-1} * A * P) * [a]_{S'}))$

---


$$(1) \quad P * [a]_{S'} = [a]_S \quad \blacksquare \quad P * [L(a)]_{S'} = [L(a)]_S$$


---

$$(2) \quad LTOverTransition \quad \blacksquare \quad [L(a)]_{S'} = P^{-1} * [L(a)]_S = P^{-1} * A * [a]_S = P^{-1} * A * P * [a]_{S'} \quad \blacksquare \quad [L(a)]_{S'} = (P^{-1} * A * P) * [a]_{S'}$$


---

$$RankNullityRelation := (Rank[A] \equiv Dim[rng_L]) \wedge (Nullity[A] \equiv Dim[ker_L]) \wedge (RankNullity \equiv RankNullityLT)$$


---

(1) TODO

---

$$SimMatrix[A, B] := \exists_P (B = P * A * P^{-1})$$


---

$$SimMatrixEquiv := (SimMatrix[A, B]) \iff (\exists_{S, T, S', T'} (([L(a)]_T = A * [a]_S) \wedge ([L(a)]_{T'} = B * [a]_{S'})))$$


---

(1) TODO

---

$$SimRank := (SimMatrix[A, B]) \implies (Rank[A] = Rank[B])$$


---

(1) TODO

---

### 3.10 Determinants

$$Perm[\sigma, S] := Bij[\sigma, S, S]$$

$$IntPermSet[S_n, n] := S_n = \{\sigma \mid Perm[\sigma, \mathbb{N}_{1,n}]\}$$

$$IntPermSetCard := (IntPermSet[S_n, n]) \implies (|S_n| = n!)$$


---

$$(1) \quad |S_1| = |\{(1)\}| = 1 = 1!$$


---

$$(2) \quad (|S_m| = m!) \implies \dots$$


---

$$(2.1) \quad |S_{m+1}| = |\mathbb{N}_{1,m+1} \times S_m| = (m+1)(m!) = (m+1)!$$


---

$$(3) \quad (|S_m| = m!) \implies (|S_{m+1}| = (m+1)!)$$


---

$$(4) \quad S_n = \{\sigma \mid Perm[\sigma, \mathbb{N}_{1,n}]\}$$


---

$$IntPermGroup := Group[S_n, \circ]$$


---

$$(1) \quad Perm[I_n, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \quad \blacksquare \quad I_n \in S_n$$


---

$$(2) \quad (\sigma, \tau, v \in S_n) \implies \dots$$


---

$$(2.1) \quad (Bij[\sigma, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \wedge (Bij[\tau, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}]) \quad \blacksquare \quad Bij[\sigma \circ \tau, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \quad \blacksquare \quad \sigma \circ \tau \in S_n$$


---

$$(2.2) \quad (Bij[\sigma, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \wedge (Bij[\tau, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}]) \wedge (Bij[v, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}]) \quad \blacksquare \quad (\sigma \circ \tau) \circ v = \sigma \circ (\tau \circ v)$$


---

$$(2.3) \quad \sigma \circ I_n = \sigma = I_n \circ \sigma$$


---

$$(2.4) \quad Bij[\sigma, \mathbb{N}_{1,n}, \mathbb{N}_{1,n}] \quad \blacksquare \quad \sigma \circ \sigma^{-1} = I_n = \sigma^{-1} \circ \sigma$$


---

$$(3) \quad Group[S_n, \circ]$$


---

$$IntPermSetEquiv := (IntPermSet[S_n, n]) \wedge (\tau \in S_n) \implies (S_n = \{\tau \circ \sigma \mid \sigma \in S_n\} = \{\sigma \circ \tau \mid \sigma \in S_n\} = \{\sigma^{-1} \mid \sigma \in S_n\})$$


---

$$(1) \quad (\alpha \in S_n) \iff (\alpha = \tau \circ (\tau^{-1} \circ \alpha) \in S_n) \iff (\alpha \in \{\tau \circ \sigma \mid \sigma \in S_n\})$$


---

$$(2) \quad (\alpha \in S_n) \iff (\alpha = (\alpha \circ \tau^{-1}) \circ \tau \in S_n) \iff (\alpha \in \{\sigma \circ \tau \mid \sigma \in S_n\})$$


---

$$(3) \quad (\alpha \in S_n) \iff (\alpha = (\alpha^{-1})^{-1} \in S_n) \iff (\alpha \in \{\sigma^{-1} \mid \sigma \in S_n\})$$


---

$$(4) \quad S_n = \{\tau \circ \sigma \mid \sigma \in S_n\} = \{\sigma \circ \tau \mid \sigma \in S_n\} = \{\sigma^{-1} \mid \sigma \in S_n\}$$


---

$$Inversions[n(\sigma), \sigma] := (\sigma \in S_n) \wedge (n(\sigma) = |\{(i, j) \mid (i < j) \wedge (\sigma(i) > \sigma(j))\}| = \sum_{i=1}^n (|\{(i, j) \mid (\sigma(i) > \sigma(j)) \wedge (i < j \leq n)\}|))$$

$$Transposition[\tau, m, r] := (\tau \in S_n) \wedge (\forall_{i \in \mathbb{N}_{1,n}} ((i \notin \{m, r\}) \implies (\tau(i) = i))) \wedge (\tau(m) = r) \wedge (\tau(r) = m)$$

$$TranspositionInv := (Transposition[\tau]) \implies (\tau = \tau^{-1})$$


---

$$(1) \quad \tau \circ \tau^{-1} = I_n \quad \blacksquare \quad \tau = \tau^{-1}$$


---

$$TranspositionDecomp := (\sigma \in S_n) \implies (\exists_T ((Transpositions[T]) \wedge (\sigma = \circ_{\tau_i \in T} (\tau_i))))$$

(1)	$(n(\sigma) = 0) \implies \dots$
(1.1)	$\sigma = I_n$
(1.2)	$(\text{Transpositions}[\langle(12), (12)\rangle]) \wedge (\sigma = I_n = (12) \circ (12))$
(1.3)	$\exists_T((\text{Transpositions}[T]) \wedge (\sigma = \circ_{\tau_i \in T}(\tau_i)))$
(2)	$(n(\sigma) = 0) \implies (\exists_T((\text{Transpositions}[T]) \wedge (\sigma = \circ_{\tau_i \in T}(\tau_i))))$
(3)	$((n(\sigma) = k + 1) \wedge (\forall_{\sigma' \in S_n}((n(\sigma') \leq k) \implies (\exists_T((\text{Transpositions}[T]) \wedge (\sigma' = \circ_{\tau_i \in T}(\tau_i))))))) \implies \dots$
(3.1)	$n(\sigma) = k + 1 \quad \blacksquare \quad n(\sigma) > 1 \quad \blacksquare \quad \exists_{l \in \mathbb{N}}((\sigma(l) \neq l) \wedge (\forall_{i \in \mathbb{N}_{1,l}}(\sigma(i) = i)))$
(3.2)	$\text{Transposition}[\delta, l, \tau(l)] \quad \blacksquare \quad n(\delta \circ \sigma) < n(\sigma)$
(3.3)	$\forall_{\sigma' \in S_n}((n(\sigma') \leq k) \implies (\exists_T((\text{Transpositions}[T]) \wedge (\sigma' = \circ_{\tau_i \in T}(\tau_i)))) \quad \blacksquare \quad \exists_{T'}((\text{Transpositions}[T']) \wedge (\delta \circ \sigma = \circ_{\tau_i \in T'}(\tau_i)))$
(3.4)	$\sigma = \delta^{-1} \circ \circ_{\tau_i \in T'}(\tau_i) = \delta \circ \circ_{\tau_i \in T'}(\tau_i) = \circ_{\tau_i \in T''}(\tau_i)$
(3.5)	$\exists_{T''}((\text{Transpositions}[T'']) \wedge (\sigma = \circ_{\tau_i \in T''}(\tau_i)))$
(4)	$((n(\sigma) = k + 1) \wedge (\forall_{\sigma' \in S_n}((n(\sigma') \leq k) \implies (\exists_T((\text{Transpositions}[T]) \wedge (\sigma' = \circ_{\tau_i \in T}(\tau_i))))))) \implies \dots$
(5)	$\dots (\exists_{T''}((\text{Transpositions}[T'']) \wedge (\sigma = \circ_{\tau_i \in T''}(\tau_i))))$
(6)	$\text{Induction} \quad \blacksquare \quad \exists_T((\text{Transpositions}[T]) \wedge (\sigma = \circ_{\tau_i \in T}(\tau_i)))$