

# Contents

<b>1</b>	<b>Graph Theory</b>	<b>3</b>
1.1	Graphs	3
1.1.1	**Graph operations**	3
1.1.2	Graphs	3
1.1.3	Paths, Cycles, Trails	4
1.1.4	Vertex Degrees and Counting	9
1.1.5	Trees	10
<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



# Chapter 1

## Graph Theory

### 1.1 Graphs

#### 1.1.1 \*\*Graph operations\*\*

$$\text{GraphPower}[G^r, r, G] := (V = V(G)) \wedge (E = \{\{x, y\} \mid d(x, y) \leq r\}) \wedge (G^r = (V, E))$$

$$\text{GraphSum}[G_1 + G_2, G_1, G_2] := (V = V(G_1) \cup V(G_2)) \wedge (E = E(G_1) \cup E(G_2) \cup \{\{x, y\} \mid (x \in V(G_1)) \wedge y \in V(G_2)\}) \wedge (G_1 + G_2 = (V, E))$$

$$\text{GraphCartesian}[G_1 \times G_2, G_1, G_2] := \left( \begin{array}{c} (V = V(G_1) \times V(G_2)) \\ (E = \{((x_1, y_1), (x_2, y_2)) \mid ((x_1 = x_2) \wedge (\{y_1, y_2\} \in E(G_2))) \vee ((y_1 = y_2) \wedge (\{x_1, x_2\} \in E(G_1)))\}) \\ (G_1 \times G_2 = (V, E)) \end{array} \right) \wedge$$

$$\text{GraphComposition}[G_1 \circ G_2, G_1, G_2] := \left( \begin{array}{c} (V = V(G_1) \times V(G_2)) \\ (E = \{((x_1, y_1), (x_2, y_2)) \mid ((x_1 = x_2) \wedge (\{y_1, y_2\} \in E(G_2))) \vee (\{x_1, x_2\} \in E(G_1))\}) \\ (G_1 \circ G_2 = (V, E)) \end{array} \right) \wedge$$

$$\text{GraphConjunction}[G_1 \wedge G_2, G_1, G_2] := \left( \begin{array}{c} (V = V(G_1) \times V(G_2)) \\ (E = \{((x_1, y_1), (x_2, y_2)) \mid (\{x_1, x_2\} \in E(G_1)) \wedge (\{y_1, y_2\} \in E(G_2))\}) \\ (G_1 \wedge G_2 = (V, E)) \end{array} \right) \wedge$$

$$\text{KroneckerProduct}[A \otimes B, A, B] := (\text{Matrix}[A, m, n]) \wedge (\text{Matrix}[B, p, q]) \wedge (A \otimes B = \begin{bmatrix} a_{1,1}B & \dots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \dots & a_{m,n}B \end{bmatrix} \in \mathbb{R}^{mp} \times \mathbb{R}^{nq})$$

$$\text{AdjacencyKroneckerIdentity} := \forall_{G,H} (\mathcal{A}(G \wedge H) = \mathcal{A}(H) \otimes \mathcal{A}(G))$$

(1) TODO: <https://archive.siam.org/books/textbooks/OT91sample.pdf>, etc.

#### 1.1.2 Graphs

$$\text{SimpleGraph}[(V, E)] := (\text{Set}[V]) \wedge (E \subseteq \{\{a, b\} \in V^{\{2\}} \mid a \neq b\})$$

$$\text{VertexSet}[V((V, E)), (V, E)] := (\text{SimpleGraph}[(V, E)]) \wedge (V((V, E)) = V)$$

$$\text{EdgeSet}[E((V, E)), (V, E)] := (\text{SimpleGraph}[(V, E)]) \wedge (E((V, E)) = E)$$

$$\text{AdjacentV}[\{x, y\}, G] := \{x, y\} \in E(G)$$

$$\text{Incident}[e, x, y, G] := e = \{x, y\} \in E(G)$$

$$\text{Degree}[d(x), x, G] := d(x) = |\{y \in V(G) \mid \text{AdjacentV}[\{x, y\}, G]\}|$$

$$\text{Order}[n(G), G] := n(G) = |V(G)|$$

$$\text{Size}[e(G), G] := e(G) = |E(G)|$$

$$\text{ComplementG}[\bar{G}, G] := \bar{G} = (V, V^{\{2\}} \setminus (E \cup \{\{x, x\} \mid x \in V(G)\}))$$

$$\text{Clique}[X, G] := \forall_{x_1, x_2 \in X} (\text{AdjacentV}[\{x_1, x_2\}, G])$$

$$\text{IndependentSet}[X, G] := \forall_{x_1, x_2 \in X} (\neg \text{AdjacentV}[\{x_1, x_2\}, G])$$

$$\text{BipartiteG}[G] := \exists_{X,Y} ((\text{IndependentSet}[X, G]) \wedge (\text{IndependentSet}[Y, G]) \wedge (V(G) = X \dot{\cup} Y))$$

$$\text{Coloring}[\phi, C, G] := (\text{Function}[\phi, V(G), C]) \wedge (\forall_{\{x,y\} \in E(G)} (\phi(x) \neq \phi(y)))$$

$$\text{ChromaticNumber}[\chi(G), G] := \chi(G) = \min(\{|C| \mid \exists_{\phi,C} (\text{Coloring}[\phi, C, G])\})$$

$$k\text{PartiteG}[G, k] := \exists_S ((|S| = k) \wedge (\forall_{S \in \mathcal{S}} (\text{IndependentSet}[S, G])) \wedge (V(G) = \bigcup_{S \in \mathcal{S}} (S)))$$

$$\text{PartiteSets}[S, G] := (\forall_{S \in \mathcal{S}} (\text{IndependentSet}[S, G])) \wedge (V(G) = \bigcup_{S \in \mathcal{S}} (S))$$

$$\text{CompleteBipartiteG}[G, X, Y] := (\text{PartiteSets}[\{X, Y\}, G]) \wedge (E(G) = \{\{x, y\} \mid (x \in X) \wedge (y \in Y)\})$$

### 1.1.3 Paths, Cycles, Trails

$$PathG[G] := \exists_P((Ordering[P, V(G)]) \wedge (E(G) = \{\{p_i, p_{i+1}\} \mid i \in \mathbb{N}_1^{|P|-1}\}))$$

$$CycleG[G] := \exists_C((Ordering[C, V(G)]) \wedge (E(G) = \{\{c_i, c_{i+1}\} \mid i \in \mathbb{N}_1^{|C|-1}\} \cup \{c_n, c_1\}))$$

$$CompleteG[G] := \forall_{x,y \in V(G)}((x \neq y) \implies \{x, y\} \in E(G))$$

$$TriangleG[G] := (CompleteG[G]) \wedge (n(G) = 3)$$

$$Subgraph[H, G] := (V(H) \subseteq V(G)) \wedge (E(H) \subseteq E(G))$$

$$ConnectedV[\{x, y\}, G] := \exists H((Subgraph[H, G]) \wedge (PathG[H]) \wedge (\{x, y\} \subseteq V(H)))$$

$$ConnectedG[G] := \forall_{x,y \in V(G)}(ConnectedV[\{x, y\}, G])$$

$$AdjacencyMatrix[\mathcal{A}(G), G] := (Matrix[\mathcal{A}(G)], n(G), n(G)) \wedge \mathcal{A}(G)_{i,j} = \begin{cases} 1 & \{v_i, v_j\} \in E(G) \\ 0 & \{v_i, v_j\} \notin E(G) \end{cases}$$

$$IncidenceMatrix[I(G), G] := (Matrix[\mathcal{A}(G)], n(G), e(G)) \wedge I(G)_{i,j} = \begin{cases} 1 & v_i \in e_j \\ 0 & v_i \notin e_j \end{cases}$$

$$Isomorphism[\phi, G, H] := (Bijection[\phi, V(G), V(H)]) \wedge (\forall_{x,y \in V(G)}((\{x, y\} \in E(G)) \iff (\{\phi(x), \phi(y)\} \in E(H))))$$

$$Isomorphic[G, H] := \exists_\phi(Isomorphism[\phi, G, H])$$

$$IsomorphismEqRel := \forall_{G_1, G_2, G_3} \left( \begin{array}{c} (G_1 \cong G_1) \\ ((G_1 \cong G_2) \implies (G_2 \cong G_1)) \\ (((G_1 \cong G_2) \wedge (G_2 \cong G_3)) \implies (G_1 \cong G_3)) \end{array} \right)$$

(1) Bijection and composition properties

$$IsomorphismClass[G] := (G \in \mathcal{G}) \wedge (G = [G]_{\cong})$$

$$PathN[P_n, n] := (PathG[P_n]) \wedge (n(P_n) = n)$$

$$CycleN[C_n, n] := (CycleG[C_n]) \wedge (n(C_n) = n)$$

$$CompleteN[K_n, n] := (CompleteG[K_n]) \wedge (n(K_n) = n)$$

$$BicliqueRS[K_{r,s}, r, s] := (CompleteBipartiteG[K_{r,s}]) \wedge (PartiteSets[\{R, S\}, G]) \wedge (|R| = r) \wedge (|S| = s)$$

$$SelfComplementary[G] := G \cong \bar{G}$$

$$Decomposition[D, G] := (\forall_{D \in \mathcal{D}}(Subgraph[D, G])) \wedge (\forall_{e \in E(G)} \exists!_{D \in \mathcal{D}}(e \in E(D)))$$

TODO: ADD SPECIAL GRAPHS

$$Girth[girth(G), G] := (CycleLengths[L, G]) \wedge \left( girth(G) = \begin{cases} \min(L) & L \neq \emptyset \\ \infty & L = \emptyset \end{cases} \right)$$

$$Circumference[circumference(G), G] := (CycleLengths[L, G]) \wedge \left( circumference(G) = \begin{cases} \max(L) & L \neq \emptyset \\ \infty & L = \emptyset \end{cases} \right)$$

$$Automorphism[\phi, G] := (Isomorphism[\phi, G, G])$$

$$VertexTransitive[G] := \forall_{x,y \in V(G)} \exists_\phi((Automorphism[\phi, G]) \wedge (\phi(x) = y))$$

$$Walk[W, G] := (\forall_{i \in \mathbb{N}_1^{|W|-1}}(\{w_i, w_{i+1}\} \in E(G)))$$

$$EdgesWalk[E(W), W, G] := (Walk[W, G]) \wedge (E(W) = \{\{w_i, w_{i+1}\} \mid i \in \mathbb{N}_1^{|W|-1}\})$$

$$Trail[W, G] := (Walk[W, G]) \wedge (\forall_{i,j \in \mathbb{N}_1^{|W|-1}}((i \neq j) \implies (\{w_i, w_{i+1}\} \neq \{w_j, w_{j+1}\})))$$

$$uvWalk[(u, v), W, G] := (Walk[W, G]) \wedge (W_1 = u) \wedge (W_{|W|} = v)$$

$$uvTrail[(u, v), W, G] := (Trail[W, G]) \wedge (W_1 = u) \wedge (W_{|W|} = v)$$

$$uvPath[(u, v), P] := (PathG[P]) \wedge (u, v \in V(P)) \wedge (d(u) = 1 = d(v))$$

$$LengthWalk[e(W), W, G] := (Walk[W, G]) \wedge (e(W) = |E(W)|)$$

$$ClosedWalk[W, G] := (Walk[W, G]) \wedge (w_1 = w_{|W|})$$

$$OddWalk[W, G] := (Walk[W, G]) \wedge (Odd(e(W)))$$

$$EvenWalk[W, G] := (Walk[W, G]) \wedge (Even(e(W)))$$

$$WalkContainsPath[P, W, G] := (Path[P]) \wedge (Walk[W, G]) \wedge (OrderedSublist[V(P), W]) \wedge (OrderedSublist[E(P), E(W)])$$

$$WalkContainsCycle[C, W, G] := (Cycle[C]) \wedge (Walk[W, G]) \wedge (OrderedSublist[V(C), W]) \wedge (OrderedSublist[E(C), E(W)])$$

$$uvWalkContainsuvPath := (uvWalk[(x, y), W, G]) \implies (\exists_P((uvPath[(x, y), P]) \wedge (WalkContainsPath[P, W, G])))$$

(1)  $(e(W) = 0) \implies (P = (W, \emptyset)) \blacksquare WalkContainsPath[P, W, G]$

$$(2) ((e(W) > 0) \wedge (\forall_{W'}((e(W') < e(W)) \implies ((uvWalk[(x, y), W', G]) \implies (\exists_{P'}((uvPath[(x, y), P']) \wedge (WalkContainsPath[P', W', G])))))) \implies \dots$$

$$(2.1) \text{ If } W \text{ has no duplicate vertices, then } P = W \quad \blacksquare \quad WalkContainsPath[P, W, G]$$

$$(2.2) \text{ If } W \text{ has duplicate vertices, then delete the duplicate vertices and edges between extra copies of unique vertices. This shorter } uvWalk \text{ } W' \text{ has a } uvPath \text{ } P' \text{ by IH. } \quad \blacksquare \quad WalkContainsPath[P', W, G]$$

$$(3) ((e(W) > 0) \wedge (\forall_{W'}((e(W') < e(W)) \implies ((uvWalk[(x, y), W', G]) \implies (\exists_{P'}((uvPath[(x, y), P']) \wedge (WalkContainsPath[P', W', G])))))) \implies (WalkContainsPath[P, W, G])$$

$$(4) \text{ By induction: } (uvWalk[(x, y), W, G]) \implies (\exists_P((uvPath[(x, y), P]) \wedge (WalkContainsPath[P, W, G])))$$

$$ConnectedV[(x, y), G] := \exists_P((Subgraph[P, G]) \wedge (uvPath[(x, y), P]))$$

$$Connected[G] := \forall_{x, y \in V(G)}(ConnectedV[(x, y), G])$$

$$Connection[C_G, G] := C_G = \{\langle x, y \rangle \mid ConnectedV[(x, y), G]\}$$

$$ConnectionEqRel := \forall_G \forall_{x_1, x_2, x_3 \in G} \left( \begin{array}{c} (x_1 C_G x_1) \quad \wedge \\ ((x_1 C_G x_2) \implies (x_2 C_G x_1)) \quad \wedge \\ (((x_1 C_G x_2) \wedge (x_2 C_G x_3)) \implies (x_1 \cong x_3)) \end{array} \right)$$

$$(1) \text{ By } (uvWalkContainsuvPath) \wedge (uvPath[(x, y), W]) \iff (uvPath[(y, x), W])$$

$$ConnectedSubgraph[H, G] := (Subgraph[H, G]) \wedge (Connected[H])$$

$$Component[H, G] := ConnectedSubgraph[H, G] \wedge (\neg \exists_{K \neq H}((Subgraph[H, K]) \wedge (ConnectedSubgraph[K, G])))$$

$$Trivial[G] := E(G) = \emptyset$$

$$Isolated[v, G] := d(v) = 0$$

$$Components[\mathcal{H}, G] := Partition[\mathcal{H}, G, C_G]$$

$$NumComponents[c, G] := (Components[\mathcal{H}, G]) \wedge (c = |\mathcal{H}|)$$

$$NumComponentsBound := ((|V(G)| = n) \wedge (|E(G)| = k)) \implies (n - k \leq |\mathcal{H}|)$$

$$(1) \text{ Starting from } E(G) = \emptyset, |\mathcal{H}| = n$$

$$(2) \text{ Adding an edge would decrease the number of components by 0 or 1, so after adding } k \text{ edges, } n - k \leq |\mathcal{H}|$$

$$RemoveV[G - W, W, G] := (V(G - W) = V(G) \setminus W) \wedge (E(G - W) = \{\{x, y\} \in E(G) \mid x, y \in V(G - W)\})$$

$$RemoveE[G - E, E, G] := (V(G - E) = V(G)) \wedge (E(G - E) = E(G) \setminus E)$$

$$AddE[G + e, e, G] := (e \in V(G)^{(2)}) \wedge (V(G + e) = V(G)) \wedge (E(G + e) = E(G) \cup \{e\})$$

$$InducedSubgraph[G[T], T, G] := G[T] = G - \bar{T}$$

$$IndependentSet[S, G] := E(G[S]) = \emptyset$$

$$CutVertex[v, G] := (NumComponents[c_1, G]) \wedge (NumComponents[c_2, G - v]) \wedge (c_2 > c_1)$$

$$CutEdge[e, G] := (NumComponents[c_1, G]) \wedge (NumComponents[c_2, G - e]) \wedge (c_2 > c_1)$$

$$CutEdgeEquiv := (CutEdge[e, G]) \iff (\neg \exists_C((Subgraph[C, G]) \wedge (CycleG[C]) \wedge (e \in E(C))))$$

$$(1) \text{ Let } (Component[H, G]) \wedge (e = \{x, y\} \in E(H))$$

$$(2) (CutEdge[e, G]) \iff (CutEdge[e, H]) \iff (\neg Connected[H - e])$$

$$(3) \text{ WTS: } (Connected[H - e]) \iff (\exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (e \in E(C))))$$

$$(4) (Connected[H - e]) \implies \dots$$

$$(4.1) \exists_P((PathG[P]) \wedge (Subgraph[P, H - e])) \quad \blacksquare \quad CycleG[(V(P), E(P) \cup \{e\})] \quad \blacksquare \quad \exists_C(((CycleG[C]) \wedge Subgraph[C, G]) \wedge (e \in E(C)))$$

$$(5) (Connected[H - e]) \implies (\exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (e \in E(C))))$$

$$(6) (\exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (e \in E(C)))) \implies \dots$$

$$(6.1) Component[H, G] \quad \blacksquare \quad Connected[H]$$

$$(6.2) (u, v \in V(H)) \implies \dots$$

$$(6.2.1) \exists_P((Subgraph[P, H]) \wedge (uvPath[(u, v), P]))$$

$$(6.2.2) (e \notin E(P)) \implies \dots$$

$$(6.2.2.1) (Subgraph[P, H - e]) \quad \blacksquare \quad \exists_P((Subgraph[P, H - e]) \wedge (uvPath[(u, v), P]))$$

$$(6.2.3) (e \notin E(P)) \implies (\exists_P((Subgraph[P, H - e]) \wedge (uvPath[(u, v), P])))$$

$$(6.2.4) (e \in E(P)) \implies \dots$$

$$(6.2.4.1) P' = u - xPath + x - yCycleG + y - vPath$$

(6.2.4.2)	$(Subgraph[P', H - e]) \wedge (uvPath[(u, v), P']) \vdash \exists_P((Subgraph[P, H - e]) \wedge (uvPath[(u, v), P]))$
(6.2.5)	$(e \in E(P)) \implies (\exists_P((Subgraph[P, H - e]) \wedge (uvPath[(u, v), P])))$
(6.2.6)	$\exists_P((Subgraph[P, H - e]) \wedge (uvPath[(u, v), P]))$
(6.3)	$(u, v \in V(H)) \implies (\exists_P((Subgraph[P, H - e]) \wedge (uvPath[(u, v), P]))) \vdash Connected[H - e]$
(7)	$(\exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (e \in E(C)))) \implies (Connected[H - e])$
(8)	$(Connected[H - e]) \iff (\exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (e \in E(C))))$

	$COWalkContainsOCycle := ((ClosedWalk[W, G]) \wedge (OddWalk[W, G])) \implies (\exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C)))))$
(1)	$(e(W) = 1) \implies (C = (\{w_1\}, \emptyset) \vdash \exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C)))))$
(2)	$((e(W) > 1) \wedge (\forall_{W'}((e(W') < e(W)) \implies (((ClosedWalk[W', G]) \wedge (OddWalk[W', G])) \implies (\exists_{C'}((WalkContainsCycle[C', W', G]) \wedge (Odd(e(C')))))))) \implies \dots$
(2.1)	If $W$ has no repeated vertex other than the first and last, then $C = (W, E(W)) \vdash \exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C))))$
(2.2)	If $W$ has a repeated vertex $v$ , then ...
(2.2.1)	Break $W$ into two $v$ Walks $W_1, W_2$ . Since $W$ is odd, $W_1, W_2$ are odd and even walks (not in order).
(2.2.2)	WLOG let $W_1$ be the odd subwalk, then by IH $\exists_{C'}((WalkContainsCycle[C', W_1, G]) \wedge (Odd(e(C'))))$
(2.2.3)	$\exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C))))$
(2.3)	If $W$ has a repeated vertex $v$ , then $\exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C))))$
(2.4)	$\exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C))))$
(3)	$((e(W) > 1) \wedge (\forall_{W'}((e(W') < e(W)) \implies (((ClosedWalk[W', G]) \wedge (OddWalk[W', G])) \implies (\exists_{C'}((WalkContainsCycle[C', W', G]) \wedge (Odd(e(C')))))))) \implies (\exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C)))))$
(4)	By induction: $\exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C))))$

$Bipartiton[\{X, Y\}, G] := PartiteSets[\{X, Y\}, G]$   
 $ConnectedBipartite[G] := \exists!_{\{X, Y\}}(Bipartiton[\{X, Y\}, G])$

$BipartiteEquiv := (Bipartite[G]) \iff (\neg \exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (Odd(e(C)))))$

(1)	$(Bipartite[G]) \implies \dots$
(1.1)	Every step alternates between each bipartition. Thus the end vertex of the odd walk cannot be the start vertex, and it is not a cycle.
(1.2)	$\neg \exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (Odd(e(C))))$
(2)	$(Bipartite[G]) \implies (\neg \exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (Odd(e(C)))))$
(3)	$(\neg \exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (Odd(e(C))))) \implies \dots$
(3.1)	Consider each nontrivial component $H$ , and pick a $u \in V(H)$ .
(3.2)	Let $X = \{v \in H \mid Even(d(v, u))\}$ and let $Y = \{v \in H \mid Odd(d(v, u))\}$ .
(3.3)	Suppose $X$ or $Y$ are not independent sets. WLOG choose $X$ .
(3.3.1)	$X$ must contain an edge - call it $\{v, v'\}$
(3.3.2)	A closed odd walk could be: min u-v path (+ even) and v-v' (+ 1) and min v'-u path (+ even)
(3.3.3)	By $COWalkContainsOCycle$ , there exists an odd cycle in $G$ . $\vdash \perp$
(3.4)	$X$ and $Y$ are independent sets; furthermore $X, Y$ are bipartitions of $G$ . $\vdash Bipartite[G]$
(4)	$(\neg \exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (Odd(e(C))))) \implies (Bipartite[G])$
(5)	$(Bipartite[G]) \iff (\neg \exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (Odd(e(C)))))$

$UnionG[\cup(G), G] := (V(\cup(G)) = \bigcup_{G \in \mathcal{G}} (V(G))) \wedge (E(\cup(G)) = \bigcup_{G \in \mathcal{G}} (E(G)))$

$CompleteAsBipartiteUnion := (\exists_{\langle B \rangle_1^k} (\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B]) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \iff (n \leq 2^k)$

(1)	$(k = 1) \implies \dots$
(1.1)	$(\exists_{\langle B \rangle_1^k} (\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B]) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \iff (Bipartite[K_n])$
(1.2)	$(n \leq 2^k) \implies \dots$
(1.2.1)	$n \leq 2^1 = 2 \vdash ((n = 1) \vee (n = 2))$
(1.2.2)	$(BipartiteG[K_1]) \wedge (BipartiteG[K_2]) \vdash Bipartite[K_n]$
(1.3)	$(n \leq 2^k) \implies (Bipartite[K_n])$
(1.4)	$(Bipartite[K_n]) \implies \dots$

(1.4.1)	$(n > 2) \implies \dots$
(1.4.1.1)	$K_n$ has an odd cycle
(1.4.1.2)	$BipartiteEquiv$ and $K_n$ has an odd cycle $\blacksquare \neg Bipartite[K_n] \blacksquare \perp$
(1.4.2)	$(n > 2) \implies (\perp) \blacksquare n \leq 2$
(1.5)	$(Bipartite[K_n]) \implies (n \leq 2)$
(1.6)	$(Bipartite[K_n]) \iff (n \leq 2) \blacksquare (\exists_{\langle B \rangle_1^k} ((\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \iff (n \leq 2)$
(2)	$(k = 1) \implies ((\exists_{\langle B \rangle_1^k} ((\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \iff (n \leq 2))$
(3)	$((k > 1) \wedge (\forall_{k'} ((k' < k) \implies ((\exists_{\langle B \rangle_1^{k'}} ((\forall_{B \in \langle B \rangle_1^{k'}} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^{k'}]))) \iff (n \leq 2^{k'})))) \implies \dots$
(3.1)	$(\exists_{\langle B \rangle_1^k} ((\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \implies \dots$
(3.1.1)	$K_n = \cup(\langle B \rangle_1^k) = \bigcup_{i=1}^k (B_i) = \bigcup_{i=1}^{k-1} (B_i) \cup B_k \blacksquare K_n = \bigcup_{i=1}^{k-1} (B_i) \cup B_k$
(3.1.2)	$Bipartite[B_k] \blacksquare \exists_{X_0, Y_0} (PartiteSets[\{X_0, Y_0\}, B_k]) \blacksquare \exists_{X, Y} (PartiteSets[\{X, Y\}, (V(G), E(B_k))])$
(3.1.3)	$K_n = (\bigcup_{i=1}^{k-1} (B_i) \cup B_k) \wedge (PartiteSets[\{X, Y\}, B_k]) \blacksquare \bigcup_{i=1}^{k-1} (B_i) = K_n[X] \cup K_n[Y]$
(3.1.4)	$\bigcup_{i=1}^{k-1} (B_i) = K_n[X] \cup K_n[Y]$ and IH $\blacksquare ( X  = n(K_n[X]) \leq 2^{k-1}) \wedge ( Y  = n(K_n[Y]) \leq 2^{k-1})$
(3.1.5)	$n =  G  =  X  +  Y  \leq 2^{k-1} + 2^{k-1} = 2^k \blacksquare n \leq 2^k$
(3.2)	$(\exists_{\langle B \rangle_1^k} ((\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \implies (n \leq 2^k)$
(3.3)	$(n \leq 2^k) \implies \dots$
(3.3.1)	$\exists_{X, Y} ((X \dot{\cup} Y = V(K_n)) \wedge ( X  \leq 2^{k-1}) \wedge ( Y  \leq 2^{k-1}))$
(3.3.2)	$\text{IH} \blacksquare (\exists_{\langle X \rangle_1^{k-1}} ((\forall_{X \in \langle X \rangle_1^{k-1}} (BipartiteG[X])) \wedge (UnionG[K_n[X], \langle X \rangle_1^{k-1}])) \wedge (\exists_{\langle Y \rangle_1^{k-1}} ((\forall_{Y \in \langle Y \rangle_1^{k-1}} (BipartiteG[Y])) \wedge (UnionG[K_n[Y], \langle Y \rangle_1^{k-1}]))))$
(3.3.3)	$(\langle Z \rangle_1^{k-1} = \langle X_i \cup Y_i \rangle_{i=1}^{k-1}) \wedge (CompleteBipartiteG[Z_k, X, Y]) \blacksquare (\forall_{Z \in \langle Z \rangle_1^k} (BipartiteG[Z])) \wedge (UnionG[K_n, \langle Z \rangle_1^k])$
(3.4)	$(n \leq 2^k) \implies (\exists_{\langle B \rangle_1^k} ((\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^k])))$
(3.5)	$(\exists_{\langle B \rangle_1^k} ((\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \iff (n \leq 2^k)$
(4)	$((k > 1) \wedge (\forall_{k'} ((k' < k) \implies ((\exists_{\langle B \rangle_1^k} ((\langle B \rangle_1^k = k') \wedge (\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \iff (n \leq 2^{k'})))) \implies (\exists_{\langle B \rangle_1^k} ((\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \iff (n \leq 2)$
(5)	By induction: $(\exists_{\langle B \rangle_1^k} ((\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B])) \wedge (UnionG[K_n, \langle B \rangle_1^k]))) \iff (n \leq 2)$

$Circuit[W, G] := (Trail[W, G]) \wedge (ClosedWalk[W, G])$   
 $EulerianTrail[W, G] := ((Trail[W, G]) \wedge (E(W) = E(G)))$   
 $EulerianCircuit[W, G] := ((Circuit[W, G]) \wedge (E(W) = E(G)))$   
 $Eulerian[G] := \exists_W (EulerianCircuit[W, G])$

$OddVertex[v, G] := Odd(d(v))$   
 $EvenVertex[v, G] := Even(d(v))$   
 $EvenGraph[G] := \forall_{v \in V(G)} (EvenVertex[v, G])$

$MaximalPath[P, G] := (Subgraph[P, G]) \wedge (PathG[P]) \wedge (\neg \exists_{P' \neq P} ((Subgraph[P, P']) \wedge (Subgraph[P', G]) \wedge (PathG[P'])))$   
 $MaximalTrail[W, G] := (Trail[W, G]) \wedge (\neg \exists_{W' \neq W} ((W \subseteq W') \wedge (Trail[W', G])))$

$VertexDegreeCycle := (\forall_{v \in V(G)} (2 \leq d(v))) \implies (\exists_C ((Subgraph[C, G]) \wedge (CycleG[C])))$

- (1)  $\exists_P (MaximalPath[P, G]) \blacksquare \exists_{u, v} (uvPath[(u, v), P])$
- (2) Since  $P$  is maximal, adjacent vertices of  $u$  must be contained in  $P$ .
- (3) Since  $2 \leq d(u)$ , then  $u$  has at least 2 edges that are incident among the vertices in  $P$ .
- (4) These edges form a cycle from  $u$ .  $\exists_C ((Subgraph[C, G]) \wedge (CycleG[C]))$ .

$$EulerianEquiv := (Components[\mathcal{H}, G]) \implies ((Eulerian[G]) \iff (((\exists H \in \mathcal{H}) (\neg Trivial[H])) \wedge (EvenGraph[G])))$$

$$(1) \quad (Eulerian[G]) \implies \dots$$

$$(1.1) \quad Eulerian[G] \implies \exists W (EulerianCircuit[W, G])$$

$$(1.2) \quad \text{The first and last vertices have even degree, and the intermediate vertices have even degree.} \implies EvenGraph[G]$$

$$(1.3) \quad E(G) \text{ must be covered by the } W, \text{ thus they must lie on the same non-trivial component.} \implies ((\exists H \in \mathcal{H}) (\neg Trivial[H]))$$

$$(1.4) \quad (((\exists H \in \mathcal{H}) (\neg Trivial[H])) \wedge (EvenGraph[G]))$$

$$(2) \quad (Eulerian[G]) \implies (((\exists H \in \mathcal{H}) (\neg Trivial[H])) \wedge (EvenGraph[G]))$$

$$(3) \quad (((\exists H \in \mathcal{H}) (\neg Trivial[H])) \wedge (EvenGraph[G])) \implies \dots$$

$$(3.1) \quad (E(G) = 0) \implies \dots$$

$$(3.1.1) \quad \text{Let the Eulerian circuit be consist of just one vertex.} \implies Eulerian[G]$$

$$(3.2) \quad (E(G) = 0) \implies (Eulerian[G])$$

$$(3.3) \quad ((E(G) > 0) \wedge (\forall G' ((E(G') < E(G)) \implies (Eulerian[G']))) \implies \dots$$

$$(3.3.1) \quad \exists!_H (H \in \mathcal{H} \mid \neg Trivial[H])$$

$$(3.3.2) \quad EvenGraph[G] \implies EvenGraph[H] \implies \forall_{v \in V(H)} (2 \leq d(v))$$

$$(3.3.3) \quad VertexDegreeCycle \implies \exists_C ((Subgraph[C, H]) \wedge (CycleG[C]))$$

$$(3.3.4) \quad G' := G - E(C)$$

$$(3.3.5) \quad \text{Since the vertices in a cycle have degree 2, } EvenGraph[G']. \text{ Each } H' \text{ component of } G' \text{ is also an } EvenGraph[H'].$$

$$(3.3.6) \quad \text{By IH and } \forall_{H' \in \mathcal{H}'} (E(H') < E(G)) \implies \forall_{H' \in \mathcal{H}'} (Eulerian[H'])$$

$$(3.3.7) \quad \text{The Eulerian circuit of } G \text{ can be constructed by:}$$

$$(3.3.7.1) \quad \text{Start at some vertex in } C$$

$$(3.3.7.2) \quad \text{Go around } C, \text{ until the trail reaches a vertex of some } H' \in \mathcal{H}'$$

$$(3.3.7.3) \quad \text{Trail around } H' \text{ using it's own Eulerian trail, and return to the vertex in } C'.$$

$$(3.3.7.4) \quad \text{Continue the last two steps until the trail of } C \text{ is complete.}$$

$$(3.3.8) \quad Eulerian[G]$$

$$(3.4) \quad ((E(G) > 0) \wedge (\forall G' ((E(G') < E(G)) \implies (Eulerian[G']))) \implies (Eulerian[G]))$$

$$(4) \quad (((\exists H \in \mathcal{H}) (\neg Trivial[H])) \wedge (EvenGraph[G])) \implies (Eulerian[G])$$

$$EvenGraphCycles := (EvenGraph[G]) \implies (\exists_D ((Decomposition[D, G]) \wedge (\forall_{D \in \mathcal{D}} (Cycle[D]))))$$

$$(1) \quad (E(G) = 0) \implies \dots$$

$$(1.1) \quad \mathcal{D} = \{G\} \implies \exists_D ((Decomposition[D, G]) \wedge (\forall_{D \in \mathcal{D}} (Cycle[D])))$$

$$(2) \quad ((E(G) > 0) \wedge (\forall G' ((E(G') < E(G)) \implies ((EvenGraph[G']) \implies (\exists_{D'} ((Decomposition[D', G']) \wedge (\forall_{D' \in \mathcal{D}'} (Cycle[D']))))))) \implies \dots$$

$$(2.1) \quad (E(G) > 0) \wedge (EvenGraph[G]) \implies \forall_{v \in V(G)} (2 \leq d(v))$$

$$(2.2) \quad VertexDegreeCycle \implies \exists_C ((Subgraph[C, G]) \wedge (CycleG[C]))$$

$$(2.3) \quad G' := G - E(C)$$

$$(2.4) \quad \text{Since the vertices in a cycle have degree 2, } EvenGraph[G']. \text{ Each } D' \text{ component of } G' \text{ is also an } EvenGraph[D'].$$

$$(2.5) \quad E(D') < E(G) \text{ and IH, there exists a cycle decomposition of } D'.$$

$$(2.6) \quad \text{The cycle decomposition of } G \text{ can be constructed by collecting the cycle decompositions of all } D' \in \mathcal{D}' \text{ and including } C.$$

$$(2.7) \quad \exists_D ((Decomposition[D, G]) \wedge (\forall_{D \in \mathcal{D}} (Cycle[D])))$$

$$(3) \quad ((E(G) > 0) \wedge (\forall G' ((E(G') < E(G)) \implies ((EvenGraph[G']) \implies (\exists_{D'} ((Decomposition[D', G']) \wedge (\forall_{D' \in \mathcal{D}'} (Cycle[D']))))))) \implies (\exists_D ((Decomposition[D, G]) \wedge (\forall_{D \in \mathcal{D}} (Cycle[D]))))$$

$$(4) \quad \text{By induction, } \exists_D ((Decomposition[D, G]) \wedge (\forall_{D \in \mathcal{D}} (Cycle[D])))$$

$$VertexDegreePathk := (\forall_{v \in V(G)} (k \leq d(v))) \implies (\exists_P ((Subgraph[P, G]) \wedge (PathG[P]) \wedge (k \leq e(P))))$$

$$(1) \quad \exists_P (MaximalPath[P, G]) \implies \exists_{u,v} (uvPath[(u, v), P])$$

$$(2) \quad \text{Since } P \text{ is maximal, adjacent vertices of } u \text{ must be contained in } P.$$

$$(3) \quad \text{Since } k \leq d(u), \text{ then } u \text{ has at least } k \text{ edges that are incident among the vertices in } P.$$

$$(4) \quad \text{Thus } P \text{ has at least } k \text{ vertices.} \implies k \leq e(P).$$

$$(5) \quad \exists_P ((Subgraph[P, G]) \wedge (PathG[P]) \wedge (k \leq e(P)))$$

$$VertexDegreeCyclek := ((k \geq 2) \wedge (\forall_{v \in V(G)} (k \leq d(v)))) \implies (\exists_C ((Subgraph[C, G]) \wedge (CycleG[C]) \wedge (k + 1 \leq e(C))))$$

$$(1) \quad VertexDegreePathk \implies \exists_P ((Subgraph[P, G]) \wedge (PathG[P]) \wedge (k \leq e(P)))$$



- 
- (2) The edge formed by  $u$  and it's farthest neighbor along  $P$  will form a cycle  $C$  with  $k + 1 \leq e(C)$
- (3)  $((k \geq 2) \wedge (\forall_{v \in V(G)} (k \leq d(v)))) \implies (\exists_C ((Subgraph[C, G]) \wedge (CycleG[C]) \wedge (k + 1 \leq e(C))))$
- 

$NonCutVertices := (n(G) \geq 2) \implies (\exists_{x,y \in V(G)} ((x \neq y) \wedge (\neg CutVertex[x, G]) \wedge (\neg CutVertex[y, G])))$

- 
- (1)  $\exists_P (MaximalPath[P, G]) \blacksquare \exists_{u,v} (uvPath[(u, v), P])$
- (2)  $Connected[P - u] \blacksquare \neg CutVertex[u, G]$
- (3)  $(v \neq u) \implies (\neg CutVertex[v, G])$
- (4)  $(v = u) \implies \dots \blacksquare \text{Take another maximal path within } P - u. \blacksquare \text{Take another endpoint } u'. \blacksquare \neg CutVertex[u', G]$
- 

$EvenGraphMaximalTrailClosed := ((EvenGraph[G]) \wedge (MaximumTrail[W, G])) \implies (ClosedWalk[W, G])$

- 
- (1) Every step in  $W$  adds 1 degree to each endpoint.
- (2) Thus when arriving at a vertex  $u$  that is not the initial vertex,  $u$  will have an odd count of edges incident to it.
- (3) Since  $u$  has an even degree, then there remains an edge where  $W$  can continue.
- (4) Therefore, the  $W$  can only end (become maximal) when it reaches it's initial vertex.  $\blacksquare ClosedWalk[W, G]$
- 

$OddVertexTrailDecomposition := ((Connected[G]) \wedge (|\{v \in V(G) \mid Odd(d(v))\}| = 2k)) \implies (\exists_D ((\forall_{D \in \mathcal{D}} (Trail[D, G])) \wedge (Decomposition[D, G]) \wedge (|D| = \max(\{k, 1\}))))$

- 
- (1)  $(k = 0) \implies \dots$
- (1.1)  $k = 0 \blacksquare EvenGraph[G]$
- (1.2)  $Connected[G] \blacksquare \exists!_{H \in \mathcal{H}} (\neg Trivial[H])$
- (1.3)  $EulerianEquiv \blacksquare Eulerian[G] \blacksquare \exists_{W'} (EulerianCircuit[W', G])$
- (1.4)  $D := (V(G), E(W)) \blacksquare (Trail[D, G]) \wedge (Decomposition[\{D\}, G]) \wedge (\{D\} = 1 = \max(\{k, 1\}))$
- (2)  $(k = 0) \implies (\exists_D ((\forall_{D \in \mathcal{D}} (Trail[D, G])) \wedge (Decomposition[D, G]) \wedge (|D| = \max(\{k, 1\}))))$
- (3)  $(k > 0) \implies \dots$
- (3.1) Since each trail adds an even degree to each non-endpoint vertex, we need at least  $k$  trails to partition the  $2k$  odd vertices.
- (3.2) Partition the edges into  $k$  trails such that the ends of each trail will land on an odd vertex.
- (3.3) Construct a new graph  $G'$  where the  $k$  trails are connected by an edge.  $\blacksquare (\exists!_{H' \in \mathcal{H}'} (\neg Trivial[H'])) \wedge (EvenGraph[G'])$
- (3.4)  $EulerianEquiv \blacksquare Eulerian[G'] \blacksquare \exists_{W'} (EulerianCircuit[W', G'])$
- (3.5) Construct  $D$  to be the trails in  $W'$  separated by  $E(G) \setminus E(G')$ .  $\blacksquare (Decomposition[D, G]) \wedge (D = k)$
- (4)  $(k > 0) \implies (\exists_D ((\forall_{D \in \mathcal{D}} (Trail[D, G])) \wedge (Decomposition[D, G]) \wedge (|D| = \max(\{k, 1\}))))$
- (5)  $\exists_D ((\forall_{D \in \mathcal{D}} (Trail[D, G])) \wedge (Decomposition[D, G]) \wedge (|D| = \max(\{k, 1\})))$
- 

### 1.1.4 Vertex Degrees and Counting

$MinDegree[\delta(G), G] := \delta(G) = \min(\{d(v) \mid v \in V(G)\})$

$MinDegree[\Delta(G), G] := \Delta(G) = \max(\{d(v) \mid v \in V(G)\})$

$RegularG[G] := \delta(G) = \Delta(G)$

$kRegularG[G, k] := k = \delta(G) = \Delta(G)$

$Neighborhood[N(v), v, G] := N(v) = \{u \in V(G) \mid AdjacentV[\{u, v\}, G]\}$

$DegreeSumFormula := \sum_{v \in V(G)} (d(v)) = 2e(G)$

- 
- (1)  $\sum_{v \in V(G)} (d(v)) = \sum_{v \in V(G)} (|\{e \in E(G) \mid v \in e\}|) = 2|E(G)| = 2e(G)$
- 

$AverageDegree := \delta(G) \leq \frac{2e(G)}{n(G)} \leq \Delta(G)$

- 
- (1)  $\delta(G) \leq \frac{2e(G)}{n(G)} \leq \Delta(G)$
- 

$EvenNumberOfOddVertices := Even(|\{v \in V(G) \mid Odd(d(v))\}|)$

- 
- (1)  $DegreeSumFormula \blacksquare Even(\sum_{v \in V(G)} (d(v)))$
-

---


$$(2) \quad (Odd(|\{v \in V(G) \mid Odd(d(v))\}|)) \implies (Odd(\sum_{v \in V(G)} (d(v)))) \implies (\perp) \quad \blacksquare \quad Even(|\{v \in V(G) \mid Odd(d(v))\}|)$$


---

$$kRegularGraphSize := ((kRegularG[G, k]) \wedge (n(G) = n)) \implies (e(G) = nk/2)$$


---

$$(1) \quad DegreeSumFormula \quad \blacksquare \quad 2e(G) = \sum_{i=1}^n (d(v_i)) = \sum_{i=1}^n (k) = nk \quad \blacksquare \quad e(G) = nk/2$$


---

$$kCube[Q_k, k] := (V(Q_k) = \{0, 1\}^k) \wedge (E(Q_k) = \{\{x, y\} \mid diff(x, y) = 1\})$$

$$RegularPartiteSetSize := ((k > 0) \wedge (kRegularG[G, k]) \wedge (Bipartiton[\{X, Y\}, G])) \implies (|X| = |Y|)$$


---

$$(1) \quad kRegularG[G, k] \quad \blacksquare \quad (e(G) = 2|X|) \wedge (e(G) = 2|Y|) \quad \blacksquare \quad |X| = |Y|$$


---

### 1.1.5 Trees

$$Acyclic[G] := \neg \exists_C((Subgraph[C, G]) \wedge (CycleG[C]))$$

$$Forest[G] := Acyclic[G]$$

$$Tree[G] := (Connected[G]) \wedge (Acyclic[G])$$

$$Leaf[v, G] := d(v) = 1$$

$$SpanningSubgraph[H, G] := (Subgraph[H, G]) \wedge (V(H) = V(G))$$

$$SpanningTree[H, G] := (SpanningSubgraph[H, G]) \wedge (Tree[G])$$

$$LeafExistence := ((Tree[G]) \wedge (2 \leq n(G))) \implies (2 \leq |\{v \in V(G) \mid Leaf[v, G]\}|)$$


---

$$(1) \quad Tree[G] \quad \blacksquare \quad (Connected[G]) \wedge (Acyclic[G])$$


---

$$(2) \quad (2 \leq n(G)) \wedge (Connected[G]) \quad \blacksquare \quad \exists_e(e \in E(G)) \quad \blacksquare \quad \text{Let } P \text{ be the maximal path of } e.$$


---

$$(3) \quad \text{A maximal non-trivial path with no cycles has two endpoints.} \quad \blacksquare \quad 2 \leq |\{v \in V(G) \mid Leaf[v, G]\}|$$


---

$$LeafDeletion := ((Tree[G]) \wedge (n(G) = n) \wedge (Leaf[v, G])) \implies ((Tree[G - v]) \wedge (n(G - v) = n - 1))$$


---

$$(1) \quad Tree[G] \quad \blacksquare \quad (Connected[G]) \wedge (Acyclic[G])$$


---

$$(2) \quad \text{Since } d(v) = 1, v \text{ does not belong to any path connecting any other two } u_1, u_2 \in V(G). \quad \blacksquare \quad Connected[G - v]$$


---

$$(3) \quad \text{Since deleting a vertex cannot create a cycle.} \quad \blacksquare \quad Acyclic[G - v]$$


---

$$(4) \quad Tree[G - v]$$


---

$$TreeEquiv := (n = n(G) \geq 1) \implies \left( \begin{array}{l} (A) \quad (Tree[G]) \quad \iff \\ (B) \quad ((Connected[G]) \wedge (e(G) = n - 1)) \iff \\ (C) \quad ((Acyclic[G]) \wedge (e(G) = n - 1)) \iff \\ (D) \quad (\forall_{u,v \in V(G)} \exists!_P (uvPath[(u, v), P])) \end{array} \right)$$


---

$$(1) \quad (Tree[G]) \implies \dots [A \implies B]$$


---

$$(1.1) \quad Tree[G] \quad \blacksquare \quad Connected[G]$$


---

$$(1.2) \quad (n = 1) \implies (e(G) = 0 = n - 1)$$


---

$$(1.3) \quad ((n > 1) \wedge (\forall_{G'}(((n(G') < n) \wedge (Tree[G']))) \implies (e(G') = n(G') - 1)))) \implies \dots$$


---

$$(1.3.1) \quad LeafExistence \quad \blacksquare \quad \exists_{v \in V(G)} (Leaf[v, G])$$


---

$$(1.3.2) \quad LeafDeletion \quad \blacksquare \quad Tree[G - v]$$


---

$$(1.3.3) \quad \text{By IH, } e(G - v) = (n - 1) - 1 = n - 2$$


---

$$(1.3.4) \quad Leaf[v, G] \quad \blacksquare \quad e(G) = e(G - v) + 1 = n - 1$$


---

$$(1.4) \quad ((n > 1) \wedge (\forall_{G'}(((n(G') < n) \wedge (Tree[G']))) \implies (e(G') = n(G') - 1)))) \implies (e(G) = n - 1)$$


---

$$(1.5) \quad \text{By induction, } e(G) = n - 1 \quad \blacksquare \quad (Connected[G]) \wedge (e(G) = n - 1)$$


---

$$(2) \quad (Tree[G]) \implies ((Connected[G]) \wedge (e(G) = n - 1))$$


---

$$(3) \quad ((Connected[G]) \wedge (e(G) = n - 1)) \implies \dots [B \implies C]$$


---

$$(3.1) \quad \text{Delete all edges that form a cycle in } G \text{ to form } G'. \quad \blacksquare \quad Acyclic[G']$$


---

$$(3.2) \quad (Connected[G]) \wedge (CutEdgeEquiv) \quad \blacksquare \quad Connected[G']$$


---

$$(3.3) \quad (Connected[G']) \wedge (Acyclic[G']) \wedge ([A \implies B]) \quad \blacksquare \quad e(G') = n - 1$$


---

$$(3.4) \quad \text{By construction of } G' \text{ and } e(G) = n - 1 = e(G'), G = G'. \quad \blacksquare \quad Acyclic[G]$$


---

(3.5)	$(Acyclic[G]) \wedge (e(G) = n - 1)$
(4)	$((Connected[G]) \wedge (e(G) = n - 1)) \implies ((Acyclic[G]) \wedge (e(G) = n - 1))$
(5)	$((Acyclic[G]) \wedge (e(G) = n - 1)) \implies \dots [C \implies A]$
(5.1)	$Acyclic[G]$
(5.2)	$Components[\langle G_i \rangle_{i=1}^k, G] \blacksquare \sum_{i=1}^k (n(G_i)) = n(G) = n$
(5.3)	$\forall_{i \in \mathbb{N}_1^k} (Component[G_i, G]) \blacksquare \forall_{i \in \mathbb{N}_1^k} (Connected[G_i])$
(5.4)	$\forall_{i \in \mathbb{N}_1^k} ((Connected[G_i]) \wedge (Acyclic[G_i]))$
(5.5)	$([A \implies B]) \wedge (\forall_{i \in \mathbb{N}_1^k} ((Connected[G_i]) \wedge (Acyclic[G_i]))) \blacksquare \forall_{i \in \mathbb{N}_1^k} (e(G_i) = n(G_i) - 1)$
(5.6)	$e(G) = \sum_{i=1}^k (e(G_i)) = \sum_{i=1}^k (n(G_i) - 1) = n - k$
(5.7)	$(e(G) = n - k) \wedge (e(G) = n - 1) \blacksquare k = 1 \blacksquare Connected[G]$
(5.8)	$(Connected[G]) \wedge (Acyclic[G]) \blacksquare Tree[G]$
(6)	$((Acyclic[G]) \wedge (e(G) = n - 1)) \implies (Tree[G])$
(7)	$(Tree[G]) \implies \dots [A \implies D]$
(7.1)	$Tree[G] \blacksquare (Connected[G]) \wedge (Acyclic[G])$
(7.2)	$Connected[G] \blacksquare \forall_{u,v \in V(G)} \exists_P (uvPath[(u, v), P])$
(7.3)	$((u, v \in V(G)) \wedge (uvPath[(u, v), P_1]) \wedge (uvPath[(u, v), P_2])) \implies \dots$
(7.3.1)	$(P_1 \neq P_2) \implies \dots$
(7.3.1.1)	Take the shortest subpaths $P'_1, P'_2$ of $P_1, P_2$ that ends on the same endpoints $u', v'$ .
(7.3.1.2)	By the extremal choice, $P'_1, P'_2$ share the same endpoints, but no internal vertices. $\blacksquare Cycle[P'_1 \cup P'_2]$
(7.3.1.3)	$(Acyclic[G]) \wedge (Cycle[P'_1 \cup P'_2]) \blacksquare \perp$
(7.3.2)	$(P_1 \neq P_2) \implies (\perp) \blacksquare P_1 = P_2$
(7.4)	$((u, v \in V(G)) \wedge (uvPath[(u, v), P_1]) \wedge (uvPath[(u, v), P_2])) \implies (P_1 = P_2)$
(8)	$(Tree[G]) \implies (\forall_{u,v \in V(G)} \exists!_P (uvPath[(u, v), P]))$
(9)	$(\forall_{u,v \in V(G)} \exists!_P (uvPath[(u, v), P])) \implies \dots [D \implies A]$
(9.1)	$\forall_{u,v \in V(G)} \exists!_P (uvPath[(u, v), P]) \blacksquare \forall_{u,v \in V(G)} \exists_P (uvPath[(u, v), P]) \blacksquare Connected[G]$
(9.2)	$(\neg Acyclic[G]) \implies \dots$
(9.2.1)	$\exists_C (Cycle[C] \wedge (Subgraph[C, G]))$
(9.2.2)	$\forall_{c_1, c_2 \in C} \exists_{P, P'} ((P \neq P') \wedge (uvPath[(c_1, c_2), P]) \wedge (uvPath[(c_1, c_2), P']))$
(9.2.3)	$(\forall_{u,v \in V(G)} \exists!_P (uvPath[(u, v), P])) \wedge (\forall_{c_1, c_2 \in C} \exists_{P, P'} ((P \neq P') \wedge (uvPath[(c_1, c_2), P]) \wedge (uvPath[(c_1, c_2), P']))) \blacksquare \perp$
(9.3)	$(\neg Acyclic[G]) \implies (\perp) \blacksquare Acyclic[G]$
(9.4)	$(Connected[G]) \wedge (Acyclic[G])$
(10)	$(\forall_{u,v \in V(G)} \exists!_P (uvPath[(u, v), P])) \implies (Tree[G])$

$$TreeEquivCorollaries := \left( \begin{array}{l} (A) \ ((Tree[G]) \implies (\forall_{e \in E(G)} (CutEdge[e, G]))) \quad \wedge \\ (B) \ ((Tree[G]) \implies (\exists!_C ((Cycle[C]) \wedge (Subgraph[C, G + e])))) \wedge \\ (C) \ ((Connected[G]) \implies (\exists_T (SpanningTree[T, G]))) \end{array} \right)$$

(1)	$(Tree[G]) \implies \dots [A]$
(1.1)	$Tree[G] \blacksquare Connected[G]$
(1.2)	$TreeEquiv \blacksquare \forall_{u,v \in V(G)} \exists!_P (uvPath[(u, v), P]) \blacksquare \forall_{\{u,v\} \in E(G)} (CutEdge[\{u, v\}, G])$
(2)	$(Tree[G]) \implies (\forall_{e \in E(G)} (CutEdge[e, G]))$
(3)	$(Tree[G]) \implies \dots [B]$
(3.1)	$Tree[G] \blacksquare Connected[G]$
(3.2)	$TreeEquiv \blacksquare \forall_{u,v \in V(G)} \exists!_P (uvPath[(u, v), P]) \blacksquare \exists!_C ((Cycle[C]) \wedge (Subgraph[C, G + e]))$
(4)	$(Tree[G]) \implies (\exists!_C ((Cycle[C]) \wedge (Subgraph[C, G + e])))$
(5)	$(Connected[G]) \implies \dots [C]$
(5.1)	Delete all edges that form a cycle in $G$ to form $G'$ . $\blacksquare (Acyclic[G']) \wedge (V(G') = V(G))$
(5.2)	$V(G') = V(G) \blacksquare SpanningSubgraph[G', G]$
(5.3)	$(Connected[G]) \wedge (CutEdgeEquiv) \blacksquare Connected[G']$

---


$$(5.4) \quad (\text{Connected}[G']) \wedge (\text{Acyclic}[G']) \quad \blacksquare \quad \text{Tree}[G']$$


---

$$(5.5) \quad (\text{SpanningSubgraph}[G', G] \wedge (\text{Tree}[G']) \quad \blacksquare \quad \text{SpanningTree}[G', G] \quad \blacksquare \quad \exists_T(\text{SpanningTree}[T, G])$$


---

$$(6) \quad (\text{Connected}[G]) \implies (\exists_T(\text{SpanningTree}[T, G]))$$


---

CONTHERE p. 69

$$Walk[W, G] := (\forall_{i \in \mathbb{N}_1^{|W|}} (w_i \in V(G))) \wedge (\forall_{i \in \mathbb{N}_1^{|W|-1}} (\{v_i, v_{i+1}\} \in E(G)))$$

$$WalkEV[(x, y), (W, G)] := (Walk[W, G]) \wedge (x, y) = (w_1, w_{|W|})$$

$$WalkL[l, (W, G)] := (Walk[W, G]) \wedge (l = |W| - 1)$$

$$TrailW[W, G] := (Walk[W, G]) \wedge (\forall_{i, j \in \mathbb{N}_1^{|W|-1}} ((i \neq j) \implies (\{w_i, w_{i+1}\} \neq \{w_j, w_{j+1}\})))$$

$$PathW[W, G] := (Walk[W, G]) \wedge (\forall_{i, j \in \mathbb{N}_1^{|W|}} ((i \neq j) \implies (w_i \neq w_j)))$$

$$ClosedWalk[W, G] := (Walk[W, G]) \wedge (w_{|W|} = w_1)$$

$$Circuit[W, G] := (Trail[W, G]) \wedge (ClosedWalk[W, G])$$

$$CycleW[W, G] := (ClosedWalk[W, G]) \wedge (\forall_{i \in \mathbb{N}_2^{|W|-1}} (w_0 \neq w_i \neq w_{|W|})) \wedge (\forall_{i, j \in \mathbb{N}_2^{|W|-1}} ((i \neq j) \implies (w_i \neq w_j))) \wedge (|W| - 1 \geq 3)$$

$$CycleE[E, (W, G)] := (CycleW[W, G]) \wedge (E = \{\{w_i, w_{i+1}\} \mid i \in \mathbb{N}_1^{|W|-1}\})$$

$$EvenCycleW[W, G] := (CycleW[W, G]) \wedge (Even(|W| - 1))$$

$$OddCycleW[W, G] := (CycleW[W, G]) \wedge (Odd(|W| - 1))$$

$$TriangleW[W, G] := (CycleW[W, G]) \wedge (|W| - 1 = 3)$$

$$IndependentV[V, G] := \forall_{x, y \in V} (\neg AdjacentV[(x, y), G])$$

$$IndependentE[E, G] := \forall_{a, b \in E} (\neg AdjacentE[(a, b), G])$$

$$IndependentPathG[P, G] := \exists_{x, y \in V(G)} \forall_{P, Q \in \mathcal{P}} ((P \neq Q) \implies (V(P) \cap V(Q) = \{x, y\}))$$

$$IndependentVEquiv := IndependentV \iff (SubgraphInducedByV[] \cong E_n)$$

$$PathG[P, V] := (V(P) = V) \wedge (E(P) = \{\{v_i, v_{i+1}\} \mid i \in \mathbb{N}_1^{|V|-1}\})$$

$$CycleG[P, V] := (V(P) = V) \wedge (E(P) = \{\{v_i, v_{i+1}\} \mid i \in \mathbb{N}_1^{|V|-1}\} \cup \{v_{|V|}, v_1\})$$

$$PathInG[P, V, G] := (PathG[P, V]) \wedge (Subgraph[P, G])$$

$$PathXY[P, (x, y), V, G] := (PathInG[P, V, G]) \wedge ((v_1, v_{|V|}) = (x, y))$$

$$CycleInG[C, V, G] := (CycleG[C, V]) \wedge (Subgraph[C, G])$$

$$CyclePartition := (\forall_{v \in V(G)} (Even(d(v)))) \iff (\exists_C ((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E, (C, G)])) \wedge (Partition[\mathcal{E}, E(G)])))$$

---


$$(1) (\exists_C ((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E, (C, G)])) \wedge (Partition[\mathcal{E}, E(G)]))) \implies \dots$$


---

$$(1.1) \quad \forall_{v \in V(G)} (d(v) = 2 * |\{v \mid (C \in \mathcal{C}) \wedge (v \in C)\}|) \quad \blacksquare \quad \forall_{v \in V(G)} (Even(d(v)))$$


---

$$(2) (\exists_C ((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E, (C, G)])) \wedge (Partition[\mathcal{E}, E(G)]))) \implies (\forall_{v \in V(G)} (Even(d(v))))$$


---

$$(3) (\forall_{v \in V(G)} (Even(d(v)))) \implies \dots$$


---

$$(3.1) \quad (e(G) = 0) \implies (\exists_C ((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E, (C, G)])) \wedge (Partition[\mathcal{E}, E(G)])))$$


---

$$(3.2) \quad (e(G) \neq 0) \implies \dots$$


---

$$(3.2.1) \quad (e(G) > 0) \wedge (\forall_{v \in V(G)} (Even(d(v)))) \quad \blacksquare \quad \exists_{x_0 \in V(G)} (d(x_0) \geq 2)$$


---

$$(3.2.2) \quad \text{There exists a Path } P \text{ of maximal length with endvertices } (x_0, x_l).$$


---

$$(3.2.3) \quad (d(x_0) \geq 2) \quad \blacksquare \quad \text{Let } y \text{ be another vertex adjacent to } x_0 \text{ that is not } x_1.$$


---

$$(3.2.4) \quad \text{If } y \text{ is not in } P, \text{ then } P \text{ is not a maximal Path - contradiction.}$$


---

$$(3.2.5) \quad \text{Thus } y \text{ is in } P, \text{ and } P \text{ contains a cycle } C.$$


---

$$(3.2.6) \quad \text{Let } G' = G - E(C). \quad \blacksquare \quad (\forall_{v \in V(G')} (Even(d_{G'}(v)))) \quad \blacksquare \quad \text{Repeat on } G' \text{ until all disjoint cycles } C \text{ are found.}$$


---

$$(3.2.7) \quad \exists_C ((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E, (C, G)])) \wedge (Partition[\mathcal{E}, E(G)]))$$


---

$$(3.3) \quad (e(G) \neq 0) \implies (\exists_C ((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E, (C, G)])) \wedge (Partition[\mathcal{E}, E(G)])))$$


---

$$(3.4) \quad \exists_C ((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E, (C, G)])) \wedge (Partition[\mathcal{E}, E(G)]))$$


---

$$(4) (\forall_{v \in V(G)} (Even(d(v)))) \implies (\exists_C ((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E, (C, G)])) \wedge (Partition[\mathcal{E}, E(G)])))$$


---

$$(5) (\forall_{v \in V(G)} (Even(d(v)))) \iff (\exists_C ((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E, (C, G)])) \wedge (Partition[\mathcal{E}, E(G)])))$$


---

$$MantelThm := ((|G| = n) \wedge (e(G) > \lfloor n^2/4 \rfloor)) \implies (\exists_W (Triangle[W, G]))$$


---

$$(1) (\neg \exists_W (Triangle[W, G])) \implies \dots$$


---

$$(1.1) \quad \neg \exists_W (Triangle[W, G]) \quad \blacksquare \quad \forall_{\{x, y\} \in E(G)} (\Gamma(x) \cap \Gamma(y) = \emptyset) \quad \blacksquare \quad \forall_{\{x, y\} \in E(G)} (d(x) + d(y) \leq n)$$


---

$$(1.2) \quad \sum_{\{x, y\} \in E(G)} (d(x) + d(y)) \leq n(e(G))$$


---

$$(1.3) \quad \sum_{\{x, y\} \in E(G)} (d(x) + d(y)) = \sum_{v \in V(G)} ((d(v))^2)$$


---

$$(1.4) \quad \sum_{v \in V(G)} ((d(v))^2) \leq n(e(G)) \quad \blacksquare \quad n \sum_{v \in V(G)} ((d(v))^2) \leq n^2(e(G))$$


---

$$(1.5) \quad (SumDegrees) \wedge (CauchysInequality) \quad \blacksquare \quad (2e(G))^2 = \left( \sum_{v \in V(G)} (d(v)) \right)^2 \leq \sum_{v \in V(G)} (d(v))^2$$

$$(1.6) \quad (2e(G))^2 \leq n^2(e(G)) \quad \blacksquare \quad e(G) \leq n^2/4$$

$$(1.7) \quad (e(G) > \lfloor n^2/4 \rfloor) \wedge (e(G) \leq n^2/4) \quad \blacksquare \quad \perp$$

$$(2) \quad (\neg \exists_W (Triangle[W, G])) \implies (\perp) \quad \blacksquare \quad \exists_W (Triangle[W, G])$$

$$Distance[d(x, y), x, y, G] := d(x, y) = \min(\{e(P) \mid \exists_V (PathXY[P, (x, y), V, G])\})$$

$$DistanceMetric := \forall_{G, x, y, z} \left( ((Graph[G]) \wedge (x, y, z \in V(G))) \implies \left( \begin{array}{l} (d(x, y) \geq 0) \quad \wedge \\ ((d(x, y) = 0) \iff (x = y)) \wedge \\ (d(x, y) = d(y, x)) \quad \wedge \\ (d(x, y) + d(y, z) \geq d(x, z)) \end{array} \right) \right)$$

$$(1) \quad \text{By definition of cardinality and sets, } (d(x, y) \geq 0) \wedge (d(x, y) = 0 \iff (x = y))$$

$$(2) \quad \text{By cases:}$$

$$(2.1) \quad \text{If } y \in [ShortestPathG[x, z]], \text{ then } d(x, y) + d(y, z) = d(x, z)$$

$$(2.2) \quad \text{If } y \notin [ShortestPathG[x, z]], \text{ then } d(x, y) + d(y, z) > d(x, z)$$

$$(3) \quad \text{By cases, } d(x, y) + d(y, z) \geq d(x, z)$$

$$AcyclicG[G] := \neg \exists_C (CycleIn[C, G])$$

$$ConnectedV[(x, y), G] := \exists_{P, V} (PathXY[P, (x, y), V, G])$$

$$ConnectedG[G] := \forall_{x, y \in V(G)} ((x \neq y) \implies (ConnectedV[(x, y), G]))$$

$$ConnectedSG[H, G] := (Subgraph[H, G]) \wedge (ConnectedG[H])$$

$$Component[C, G] := (ConnectedSG[C, G]) \wedge (\neg \exists_D ((SubgraphStrict[C, D]) \wedge (ConnectedSG[D, G])))$$

$$NComponent[n, G] := n = |\{C \mid Component[C, G]\}|$$

$$CutVertex[v, G] := (v \in V(G)) \wedge (NComponent[n, G]) \wedge (NComponent[m, G - v]) \wedge (m > n)$$

$$Bridge[e, G] := (e \in E(G)) \wedge (NComponent[n, G]) \wedge (NComponent[m, G - e]) \wedge (m > n)$$

$$TreeG[G] := (AcyclicG[G]) \wedge (ConnectedG[G])$$

$$ForestG[G] := AcyclicG[G]$$

$$BipartiteG[K_{m,n}, m, n] := \exists_{X, Y} ((X \cup Y = V(K_{m,n})) \wedge (X \cap Y = \emptyset) \wedge (E(K_{m,n}) \subseteq \{\{x, y\} \mid (x \in X) \wedge (y \in Y)\}))$$

$$CompleteBipartiteG[K_{m,n}, m, n] := \exists_{X, Y} ((X \cup Y = V(K_{m,n})) \wedge (X \cap Y = \emptyset) \wedge (E(K_{m,n}) = \{\{x, y\} \mid (x \in X) \wedge (y \in Y)\}))$$

$$[Notation] \quad (K(n_1, \dots, n_r)) := CompleteRpartiteG$$

$$[Notation] \quad (K_r(t)) := K(t, \dots, t)$$

$$UnionG[G \cup H, G, H] := (V(G \cup H) = V(G) \cup V(H)) \wedge (E(G \cup H) = E(G) \cup E(H))$$

$$kG[kG, k, G] := kG = \bigcup_{i \in \mathbb{N}_1^k} (uniqueCopy(G, i))$$

$$Join[G + H, G, H, ] := (V(G + H) = V(G \cup H)) \wedge (E(G + H) = E(G \cup H) \cup \{\{g, h\} \mid (g \in V(G)) \wedge (h \in V(H))\})$$

$$ComponentEquiv := ((Component[W, G]) \wedge (x \in W)) \implies \left( \begin{array}{l} (W = \{y \in V(G) \mid \exists_{P, V} (PathXY[P, (x, y), V, G])\}) \wedge \\ (W = \{y \in V(G) \mid d(x, y) \in \mathbb{N}\}) \quad \wedge \\ ((R = \{\langle u, v \rangle \mid \{u, v\} \in E(G)\}) \wedge (W = [x]_R)) \end{array} \right)$$

# 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2.3 Groups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

## 2.4 Subgroups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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


---

## 2.5 Special Groups

### 2.5.1 Cyclic Group

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

$$Generator[g, G, *] := CyclicSubgroup[G, g, G, *]$$

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

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

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

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

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

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

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


---

### 2.5.2 Symmetric and Alternating Groups

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

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

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

### 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 
- (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)  $\mathcal{G} = \{[g] \mid g \in G\} \quad \blacksquare \quad (\text{Partition}[\mathcal{G}, G]) \wedge (|\mathcal{G}| = |\text{im}_\phi|)$
- (3)  $\text{KerMultiplicityMap} \quad \blacksquare \quad \forall_{g \in G} (|[g]| = |\text{ker}_\phi|)$
- (4)  $\text{Partition}[\mathcal{G}, G] \quad \blacksquare \quad |G| = |\mathcal{G}| |\text{ker}_\phi| = |\text{im}_\phi| |\text{ker}_\phi|$

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

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

## 2.9 Conjugacy

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

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

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

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

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

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

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

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

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

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

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

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

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

(1)	$(Hx, Hy \in G/H) \implies \dots$
(1.1)	$(NormalSubgroup[H, G, *]) \wedge (QuotientGroupLemma) \quad \blacksquare \quad \forall_{x, y, z \in G} ((\exists_{h_1, h_2 \in H} (z = h_1 x h_2 y)) \iff (\exists_{h_3 \in H} (z = h_3 xy)))$
(1.2)	$(z \in Hx \bar{*} Hy) \iff (\exists_{h_1, h_2 \in H} (z = h_1 x h_2 y)) \iff (\exists_{h_3 \in H} (z = h_3 xy)) \iff (z \in Hxy) \quad \blacksquare \quad Hx \bar{*} Hy = Hxy$
(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)	$Group[H, *] \quad \blacksquare \quad ker_{\bar{\phi}} = \{x \in G \mid \bar{\phi}(x) = He\} = \{x \in G \mid Hx = H\} = H$
-----	---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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