

# Contents



# Chapter 1

## Graph Theory

### 1.1 NotationDump

### 1.2 Graphs

$$\begin{aligned} \textit{Graph}[(V, E)] &:= (V \cap E = \emptyset) \wedge (E \subseteq V^{\{2\}}) \\ \textit{SimpleGraph}[(V, E)] &:= (\textit{Graph}[(V, E)]) \wedge (E \subseteq \{\{a, b\} \in V^{\{2\}} \mid a \neq b\}) \end{aligned}$$

$$\textit{VertexSet}[V((V, E)), (V, E)] := (\textit{Graph}[(V, E)]) \wedge (V((V, E)) = V)$$

$$\textit{EdgeSet}[E((V, E)), (V, E)] := (\textit{Graph}[(V, E)]) \wedge (E((V, E)) = E)$$

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

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

$$\textit{AdjacentE}[(e_1, e_2), G] := \exists!_{x \in V(G)} ((x \in e_1) \wedge (x \in e_2))$$

$$\text{[Notation]} \quad x \, y := \textit{adjacentV}[(x, y), G]$$

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

$$\textit{SubgraphInducedByV}[G[V'], V', G] := (E' = \{e \in E(G) \mid \exists_{a,b \in V'} (\textit{Incident}[e, a, b, G])\}) \wedge (G[V'] = (V', E'))$$

$$\textit{InducedSubgraph}[H, G] := (\textit{Subgraph}[H, G]) \wedge (\textit{SpannedBy}[H, V(H), G])$$

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

$$\textit{RemoveV}[G - W, W, G] := (W \subseteq V(G)) \wedge (\textit{SubgraphInducedByV}[G - W, V(G) \setminus W, G])$$

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

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

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

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

$$\textit{DisjointEdges}[E_G(U, W), U, W, G] := (U, W \subseteq V(G)) \wedge (U \cap W = \emptyset) \wedge (E_G(U, W) = \{e \in E(G) \mid \exists_{u \in U} \exists_{w \in W} (\textit{Incident}[e, u, w, G])\})$$

$$\textit{DisjointEdgesSize}[e_G(U, W), U, W, G] := (\textit{DisjointEdges}[E_G(U, W), U, W, G]) \wedge (e_G(U, W) = |E_G(U, W)|)$$

$$\textit{Isomorphic}[H, G] \text{ or } H \cong G := \exists_{\phi} \left( (\textit{Bijection}[\phi, V(H), V(G)]) \wedge \left( \forall_{x,y \in V(H)} ((\{x, y\} \in E(H)) \iff (\{\phi(x), \phi(y)\} \in E(G))) \right) \right)$$

$$\text{[Notation]} \quad x \in G := x \in V(G)$$

$$\text{[Notation]} \quad G^n := \textit{Order}[n, G]$$

$$\text{[Notation]} \quad G(n, m) := (\textit{Order}[n, G]) \wedge (\textit{Size}[m, G])$$

$$\textit{SizeOrderN} := \left( (\textit{Graph}[G]) \wedge (n = |G|) \wedge (m = e(G)) \right) \implies (0 \leq m \leq \binom{n}{2})$$

---

$$(1) \quad 0 \leq m \leq \sum_{i=0}^{n-1} (i) = \frac{(n-1)(n)}{2} = \binom{n}{2}$$

---

$$\textit{CompleteGraph}[K_n, n] := (|K_n| = n) \wedge \left( e(K_n) = \binom{n}{2} \right)$$

$$\textit{EmptyGraph}[E_n, n] := (|K_n| = n) \wedge (e(K_n) = 0)$$

$$\textit{TrivialGraph}[G] := G = K_1 = E_1$$

$$\textit{ComplementGraph}[\bar{G}, G] := \bar{G} = \left( V, V^{\{2\}} \setminus (E \cup \{\{x, x\} \mid x \in V(G)\}) \right)$$

$$\text{OpenNbhd}[\Gamma_G(x), x, G] := \Gamma_G(x) = \{y \in V(G) \mid \text{Adjacent}V[(y, x), G]\}$$

$$\text{ClosedNbhd}[\Gamma_G^*(x), x, G] := (\text{OpenNbhd}[\Gamma_G(x), x, G]) \wedge (\Gamma_G^*(x) = \Gamma_G(x) \cup \{x\})$$

$$\text{Degree}[d_G(x), x, G] := d_G(x) = |\Gamma_G(x)|$$

$$\text{MinDegree}[\delta(G), G] := \delta(G) = \min(\{d_G(x) \mid x \in V(G)\})$$

$$\text{MaxDegree}[\Delta(G), G] := \Delta(G) = \max(\{d_G(x) \mid x \in V(G)\})$$

$$\text{Isolated}V[v, G] := d_G(v) = 0$$

$$\text{KRegularGraph}[G, k] := k = \delta(G) = \Delta(G)$$

$$\text{RegularGraph}[G] := \exists_{k \in \mathbb{N}} (\text{KRegularGraph}[G, k])$$

$$\text{DegreeSequence}[(d_G(x_i))_1^n, G] := (\text{Order}[n, G]) \wedge \left( (d_G(x_i))_1^n = \text{sort}(\{d_G(x) \mid x \in V(G)\}) \right) \wedge (\delta(G) = d_G(x_1) \leq d_G(x_n) = \Delta(G))$$

$$\text{SumDegrees} := \sum_{v \in V(G)} (\deg(v)) = 2|E(G)|$$

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

$$\text{HandshakingLemma} := \text{Even}(|\{v \mid \text{Odd}(\deg(v))\}|)$$

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

$$\text{Walk}[V_n, n, G] := (V_n = \{v_i \in V(G) \mid i \in \mathbb{N}_1^{n+1}\}) \wedge (\forall_{i \in \mathbb{N}_1^n} (\{v_i, v_{i+1}\} \in E(G)))$$

$$\text{Path}[V_n, n, G] := (\text{Walk}[V_n, n, G]) \wedge (\forall_{i, j \in \mathbb{N}_1^{n+1}} ((i \neq j) \implies (v_i \neq v_j)))$$

$$\text{ClosedWalk}[V_n, n, G] := (\text{Walk}[V_n, n, G]) \wedge (v_{n+1} = v_1)$$

$$\text{Cycle}[V_n, n, G] := (\text{ClosedWalk}[V_n, n, G]) \wedge (n > 1)$$

$$\text{Triangle}[T, G] := \text{Cycle}[T, 3, G]$$

$$\text{Girth}[G] := \min(\{n \in \mathbb{N} \mid \exists_{V_n} (\text{Cycle}[V_n, n, G])\})$$

$$\text{Circumference}[G] := \max(\{n \in \mathbb{N} \mid \exists_{V_n} (\text{Cycle}[V_n, n, G])\})$$

$$\text{Connected}V[(x, y), G] := \exists_{n, V_n} ((\text{Path}[V_n, n, G]) \wedge ((x, y) = (v_1, v_{n+1})))$$

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

$$\text{Component}[C, G] := (\text{Subgraph}[C, G]) \wedge (\forall_{c \in V(C)} \forall_{g \in V(G)} ((g \notin V(C)) \implies (\neg \text{Connected}V[(g, c), G])))$$

$$\text{Degree}[\deg(v), v, G] := \deg(v) = |\{e \in E(G) \mid v \in e\}|$$

$$\text{Regular}[G, r] := \forall_{v \in V(G)} (\deg(v) = r)$$

$$\text{SumDeg} := \sum_{v \in V(G)} (\deg(v)) = 2|E(G)|$$

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

$$\text{OddDeg} := \text{Even}(|\{v \mid \text{Odd}(\deg(v))\}|)$$

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

$$\text{AdjacencyMatrix}[\mathcal{A}(G), G] := \mathcal{A}(G) = \left[ a_{i,j} = \begin{cases} 1 & x_i x_j \in E(G) \\ 0 & x_i x_j \notin E(G) \end{cases} \right]$$

$$\text{Path}G[P_n, n] := (V = \{v_i \mid i \in \mathbb{N}_1^n\}) \wedge (E = \{\{v_i, v_{i+1}\} \mid i \in \mathbb{N}_1^{n-1}\}) \wedge (P_n = (V, E))$$

$$\text{Cycle}G[C_n, n] := (V = V(P_n)) \wedge (E = E(P_n) \cup \{\{v_n, v_1\}\}) \wedge (C_n = (V, E))$$

$$\text{Fan}G[F_n, n] := (V = V(P_n) \cup \{v_0\}) \wedge (E = E(P_n) \cup \{\{v_0, v_i\} \mid i \in \mathbb{N}_1^n\}) \wedge (F_n = (V, E))$$

$$\text{Wheel}G[W_n, n] := (V = V(P_n) \cup \{v_0\}) \wedge (E = E(P_n) \cup \{\{v_n, v_1\}\} \cup \{\{v_0, v_i\} \mid i \in \mathbb{N}_1^n\}) \wedge (W_n = (V, E))$$

$$\text{Star}G[S_n, n] := (V = V(P_n) \cup \{v_0\}) \wedge (E = \{\{v_0, v_i\} \mid i \in \mathbb{N}_1^n\}) \wedge (S_n = (V, E))$$

$$\text{Complete}G[K_n, n] := (V = V(P_n)) \wedge (E = \{\{v_i, v_j\} \mid (i, j \in \mathbb{N}_1^n) \wedge (i \neq j)\})$$

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

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

$$SnIsoKmn := S_n \cong K_{1,n} \cong K_{n,1}$$

(1) TODO  $\phi = \dots$

$$Distance[d_G(x, y), x, y, G] := d_G(x, y) = \min \left( n \in \mathbb{N} \mid \left( \exists_{V_n} (Path[V_n, n, G]) \wedge ((v_1, v_{n+1}) = (x, y)) \right) \right)$$

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

(1) By definition of cardinality and sets,  $d_G(x, y) \geq 0$ ,  $(d_G(x, y) = 0) \iff (x = y)$ ,  $d_G(x, y) = d(y, x)$

(2) By cases:

(2.1) If  $y \in [ShortestPath[x, z]]$ , then  $d_G(x, y) + d(y, z) = d_G(x, z)$

(2.2) If  $y \notin [ShortestPath[x, z]]$ , then  $d_G(x, y) + d(y, z) > d_G(x, z)$

(3) By cases,  $d_G(x, y) + d_G(y, z) \geq d_G(x, z)$

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

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

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

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

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

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

KroneckerProperties := ...

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

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

(1) TODO

acyclic graph

$$Tree[G] := (Connected[G]) \wedge (\neg \exists_{n, V_n} (Cycle[V_n, n, G]))$$

forest -> decomponents into trees

$p = |V(G)|$   $q = |E(G)|$

$$GraphEquivalences := (Tree[G]) \iff ()$$

(1) TODO



# Chapter 2

## Abstract Algebra

### 2.1 Functions

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

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

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

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

---

(1) TODO

---

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

---

(1) TODO

---

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

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

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

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

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

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

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

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

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

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

---

(1) TODO

---

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

---

(1) TODO

---

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

---

(1) TODO

---

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

---

(1) TODO

---

## 2.2 Divisibility, Equivalence Relations, Partitions

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

---

(1) TODO

---

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

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

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

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

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

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

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

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

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

---

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

---

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

---

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

---

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

---

(1) TODO

---

## 2.3 Groups

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

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

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

---

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

---

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

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

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

---

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

---

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

---

(3.1) TODO

---

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

---

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

---

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

---

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

---



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

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

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

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

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

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

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

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

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

## 2.4 Subgroups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2.5 Special Groups

### 2.5.1 Cyclic Group

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

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

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

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

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

---


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


---


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


---


$$(3.5) \quad (g^r \in H) \wedge (0 \leq r < m) \wedge \left( \bigvee_{k \in \mathbb{Z}^+} ((k < m) \implies (g^k \notin H)) \right) \quad \blacksquare \quad r = 0$$


---


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


---


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


---


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


---


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


---


$$(5.2) \quad (Group[H, G, *]) \wedge (g^m \in H) \quad \blacksquare \quad (g^m * g^m \in H) \wedge ((g^m)^{-1} \in H)$$


---


$$(5.3) \quad \text{Induction} \quad \blacksquare \quad b = (g^m)^k \in H \quad \blacksquare \quad b \in H$$


---


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


---


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


---

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

---


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


---


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


---

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

---


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


---

## 2.5.2 Symmetric and Alternating Groups

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2.5.3 Dihedral Group

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

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

## 2.6 Lagrange's Theorem

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2.7 Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2.8 Kernel and Image Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 
- (3.3)  $\exists_{g \in G} (a * b = \phi(g)) \blacksquare a * b \in im_\phi$
- 
- (4)  $(a, b \in im_\phi) \implies (a * b \in im_\phi) \blacksquare \forall_{a, b \in im_\phi} (a * b \in im_\phi)$
- 
- (5)  $(a \in im_\phi) \implies \dots$
- 
- (5.1)  $\exists_{g_a \in G} (a = \phi(g_a))$
- 
- (5.2)  $(g_a^{-1} \in G) \wedge (InvMapsInv) \blacksquare \phi(g_a^{-1}) = \phi(g_a)^{-1} = a^{-1}$
- 
- (5.3)  $\exists_{g \in G} (a^{-1} = \phi(g)) \blacksquare a^{-1} \in im_\phi$
- 
- (6)  $(a \in im_\phi) \implies (a^{-1} \in im_\phi) \blacksquare \forall_{a \in im_\phi} (a^{-1} \in im_\phi)$
- 
- (7)  $(SubgroupEquiv) \wedge (\emptyset \neq im_\phi \subseteq H) \wedge \left( \forall_{a, b \in im_\phi} (a * b \in im_\phi) \right) \wedge \left( \forall_{a \in im_\phi} (a^{-1} \in im_\phi) \right) \blacksquare Subgroup[im_\phi, H, \diamond]$
- 

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

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

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

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

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

- 
- (1)  $(x \in (ker_\phi)g) \implies \dots$
- 
- (1.1)  $\exists_{K_x \in ker_\phi} (x = K_x * g) \blacksquare \phi(x) = \phi(K_x * g) = \phi(K_x) \diamond \phi(g) = e_H \diamond \phi(g) = \phi(g) \blacksquare \phi(x) = \phi(g)$
- 
- (2)  $(x \in (ker_\phi)g) \implies (\phi(x) = \phi(g)) \blacksquare (ker_\phi)g \subseteq \{x \in G \mid \phi(x) = \phi(g)\}$
- 
- (3)  $((x \in G) \wedge (\phi(x) = \phi(g))) \implies \dots$
- 
- (3.1)  $e_H = \phi(x) \diamond \phi(g)^{-1} = \phi(x) \diamond \phi(g^{-1}) = \phi(x * g^{-1}) \blacksquare x * g^{-1} \in ker_\phi \blacksquare x \in (ker_\phi)g$
- 
- (4)  $((x \in G) \wedge (\phi(x) = \phi(g))) \implies (x \in (ker_\phi)g) \blacksquare \{x \in G \mid \phi(x) = \phi(g)\} \subseteq (ker_\phi)g$
- 
- (5)  $((ker_\phi)g \subseteq \{x \in G \mid \phi(x) = \phi(g)\}) \wedge (\{x \in G \mid \phi(x) = \phi(g)\} \subseteq (ker_\phi)g) \blacksquare (ker_\phi)g = \{x \in G \mid \phi(x) = \phi(g)\}$
-

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

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

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

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

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

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

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

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

## 2.9 Conjugacy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2.10 Normal Subgroups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2.11 Quotient Groups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

