

Contents

1	Graph Theory	3
1.1	NotationDump	3
1.2	Graphs	3
2	Abstract Algebra	7
2.1	Functions	7
2.2	Divisibility, Equivalence Relations, Partitions	7
2.3	Groups	8
2.4	Subgroups	9
2.5	Special Groups	10
2.5.1	Cyclic Group	10
2.5.2	Symmetric and Alternating Groups	11
2.5.3	Dihedral Group	11
2.6	Lagrange's Theorem	11
2.7	Homomorphisms	12
2.8	Kernel and Image Homomorphisms	13
2.9	Conjugacy	15
2.10	Normal Subgroups	16
2.11	Quotient Groups	17

Chapter 1

Graph Theory

1.1 NotationDump

1.2 Graphs

$Graph[(V, E)] := (V \cap E = \emptyset) \wedge (E \subseteq V^{\{2\}})$
 $SimpleGraph[(V, E)] := (Graph[(V, E)] \wedge (E \subseteq \{\{a, b\} \in V^{\{2\}} \mid a \neq b\}))$
 $VertexSet[V((V, E)), (V, E)] := (Graph[(V, E)] \wedge (V((V, E)) = V)$
 $EdgeSet[E((V, E)), (V, E)] := (Graph[(V, E)] \wedge (E((V, E)) = E)$
 $AdjacentV[(x, y), G] := \{x, y\} \in E(G)$
 $Incident[e, x, y, G] := e = \{x, y\} \in E(G)$
 $AdjacentE[(a, b), G] := \exists!_{x \in V(G)} ((x \in a) \wedge (x \in b))$

[Notation] $x \ y := AdjacentV[(x, y), G]$

$Subgraph[H, G] := (V(H) \subseteq V(G)) \wedge (E(H) \subseteq E(G))$
 $SubgraphInducedByV[G[V'], V', G] := (E' = \{e \in E(G) \mid \exists_{a, b \in V'} (Incident[e, a, b, G])\}) \wedge (G[V'] = (V', E'))$
 $InducedSubgraph[H, G] := (Subgraph[H, G]) \wedge (SpannedBy[H, V(H), G])$
 $SpanningSubgraph[H, G] := (Subgraph[H, G]) \wedge (V(H) = V(G))$

$RemoveV[G - W, W, G] := (W \subseteq V(G)) \wedge (SubgraphInducedByV[G - W, V(G) \setminus W, G])$
 $RemoveE[G - E, E, G] := (E \subseteq E(G)) \wedge (G - E = (V(G), E(G) \setminus E))$
 $AddE[G + e, e, G] := (e \notin E(G)) \wedge (e \in V(G)^{\{2\}}) \wedge (G + e = (V(G), E(G) \cup \{e\}))$

$Order[|G|, G] := |G| = |V(G)|$
 $Size[e(G), G] := e(G) = |E(G)|$
 $DisjointEdges[E_G(U, W), U, W, G] := (U, W \subseteq V(G)) \wedge (U \cap W = \emptyset) \wedge (E_G(U, W) = \{e \in E(G) \mid \exists_{u \in U} \exists_{w \in W} (Incident[e, u, w, G])\})$
 $DisjointEdgesSize[e_G(U, W), U, W, G] := (DisjointEdges[E_G(U, W), U, W, G]) \wedge (e_G(U, W) = |E_G(U, W)|)$
 $Isomorphic[H, G] \text{ or } H \cong G := \exists_{\phi} ((Bijection[\phi, V(H), V(G)]) \wedge (\forall_{x, y \in V(H)} ((\{x, y\} \in E(H)) \iff (\{\phi(x), \phi(y)\} \in E(G))))$

[Notation] $x \in G := x \in V(G)$

[Notation] $G^n := Order[n, G]$

[Notation] $G(n, m) := (Order[n, G]) \wedge (Size[m, G])$

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

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

$CompleteGraph[K_n, n] := (|K_n| = n) \wedge (e(K_n) = \binom{n}{2})$
 $EmptyGraph[E_n, n] := (|K_n| = n) \wedge (e(K_n) = 0)$
 $TrivialGraph[G] := G = K_1 = E_1$
 $ComplementGraph[\bar{G}, G] := \bar{G} = (V, V^{\{2\}} \setminus (E \cup \{\{x, x\} \mid x \in V(G)\}))$
 $OpenNbhd[\Gamma_G(x), x, G] := \Gamma_G(x) = \{y \in V(G) \mid AdjacentV[(y, x), G]\}$
 $ClosedNbhd[\Gamma_G^*(x), x, G] := (OpenNbhd[\Gamma_G(x), x, G]) \wedge (\Gamma_G^*(x) = \Gamma_G(x) \cup \{x\})$
 $Degree[d_G(x), x, G] := d_G(x) = |\Gamma_G(x)|$
 $MinDegree[\delta(G), G] := \delta(G) = \min(\{d_G(x) \mid x \in V(G)\})$
 $MaxDegree[\Delta(G), G] := \Delta(G) = \max(\{d_G(x) \mid x \in V(G)\})$
 $IsolatedV[v, G] := d_G(v) = 0$

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

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

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

$$SumDegrees := \sum_{v \in V(G)} (d_G(v)) = 2e(G)$$

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

$$HandshakingLemma := \sum_{v \in V(G)} (d_G(v)) \equiv 0 \pmod{2}$$

$$(1) \quad SumDegrees \quad \blacksquare \quad \sum_{v \in V(G)} (d_G(v)) = 2e(G) \quad \blacksquare \quad \exists_{k \in \mathbb{Z}} (\sum_{v \in V(G)} (d_G(v)) - 0 = 2k) \quad \blacksquare \quad \sum_{v \in V(G)} (d_G(v)) \equiv 0 \pmod{2}$$

$$DegreeCorollaries := (Even(|\{v \in V(G) \mid Odd(d_G(v))\}|)) \wedge (\delta(G) \leq \lfloor 2e(G)/n \rfloor) \wedge (\Delta(G) \geq \lceil 2e(G)/n \rceil)$$

$$(1) \quad HandshakingLemma \quad \blacksquare \quad Even(|\{v \in V(G) \mid Odd(d_G(v))\}|)$$

$$(2) \quad SumDegrees \quad \blacksquare \quad (\delta(G) \leq \lfloor 2e(G)/n \rfloor) \wedge (\Delta(G) \geq \lceil 2e(G)/n \rceil)$$

$$PathG[G, l, (x_i)_0^l] := (V(G) = \{x_i \mid i \in \mathbb{N}_0^l\}) \wedge (E(G) = \{\{x_i, x_{i+1}\} \mid i \in \mathbb{N}_0^{l-1}\})$$

$$PathEV[(a, b), (G, l, (x_i)_0^l)] := (PathG[G, l, (x_i)_0^l]) \wedge ((a, b) = (x_0, x_l))$$

$$PathL[L, (G, l, (x_i)_0^l)] := (PathG[G, l, (x_i)_0^l]) \wedge (L = e(G))$$

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

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

$$IndependentPath[P, G] := \exists_{x, y \in V(G)} \forall_{P_1, P_2 \in P} ((PathEV[(x, y), P_1]) \wedge (PathEV[(x, y), P_2]) \wedge ((P_1 \neq P_2) \implies (V(P_1) \cap V(P_2) = \{x, y\})))$$

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

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

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

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

$$Triangle[T, G] := Cycle[T, 3, G]$$

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

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

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

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

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

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

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

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

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

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

$$(1) \quad SumDeg$$

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

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

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

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

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

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

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

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

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

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

(1) TODO $\phi = \dots$

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

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

(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, $d_G(x, y) + d_G(y, z) \geq d_G(x, z)$

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

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

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

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

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

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

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

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

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

(1) TODO

Chapter 2

Abstract Algebra

2.1 Functions

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

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

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

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

(1) TODO

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

(1) TODO

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

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

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

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

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

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

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

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

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

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

(1) TODO

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

(1) TODO

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

(1) TODO

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

(1) TODO

2.2 Divisibility, Equivalence Relations, Partitions

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

(1) TODO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3 Groups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.8 Kernel and Image Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.9 Conjugacy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.10 Normal Subgroups

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

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

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

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

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

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

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

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

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

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

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

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

2.11 Quotient Groups

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

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

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

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

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

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

(1.2)	$(NormalSubgroup[H, G, *]) \wedge (x^{-1} \in G) \wedge (h_2 \in H) \quad \blacksquare \quad (x^{-1})^{-1} h_2 x^{-1} = x h_2 x^{-1} \in H$
(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)	$Group[H, *] \quad \blacksquare \quad ker_{\bar{\phi}} = \{x \in G \mid \bar{\phi}(x) = He\} = \{x \in G \mid Hx = H\} = H$
-----	---

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

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

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

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

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

(4) *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) $(g, h \in G) \implies \dots$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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