Contents

Chapter 1

Graph Theory

1.1 Graphs

$SimpleGraph[(V,E)] := (Set[V]) \wedge (E \subseteq \{\{a,b\} \in V^{\{2\}} \mid a \neq b\})$
$VertexSet[V((V,E)),(V,E)] := (SimpleGraph[(V,E)]) \wedge (V((V,E)) = V)$
$EdgeSet[E((V,E)),(V,E)] := (GrSimpleGraphaph[(V,E)]) \wedge (E((V,E)) = E)$
$AdjacentV[\{x,y\},G] := \{x,y\} \in E(G)$
$Incident[e,x,y,G] := e = \{x,y\} \in E(G)$

$ComplementG[\bar{G},G] := \bar{G} = (V, V^{\{2\}} \setminus (E \cup \{\{x,x\} \mid x \in V(G)\}))$
$Clique[X,G] := \forall_{x_1,x_2 \in X}(AdjacentV[\{x_1,x_2\},G])$
$IndependentSet[X,G] := \forall_{x_1,x_2 \in X}(\neg AdjacentV[\{x_1,x_2\},G])$
$BipartiteG[G] := \exists_{X,Y}((IndependentSet[X,G]) \wedge (IndependentSet[Y,G]) \wedge (V(G) = X \dot\cup Y))$
$Coloring[\phi,C,G] := (Function[\phi,V(G),C]) \wedge (\forall_{\{x,y\} \in E(G)}(\phi(x) \neq \phi(y)))$
$ChromaticNumber[\chi(G),G] := \chi(G) = min(\{|C| \mid \exists_{\phi,C}(Coloring[\phi,C,G])\})$

$kPartiteG[G,k] := \exists_S((|S| = k) \wedge (\forall_{S \in \mathcal{S}}(IndependentSet[S,G])) \wedge (V(G) = \overset{.}{\underset{S \in \mathcal{S}}{\bigcup}}(S)))$

$PartiteSets[S,G] := (\forall_{S \in \mathcal{S}}(IndependentSet[S,G])) \wedge (V(G) = \overset{.}{\underset{S \in \mathcal{S}}{\bigcup}}(S))$
$CompleteBipartiteG[G] := (PartiteSets[\{X,Y\},G]) \wedge (E(G) = \{\{x,y\} \mid (x \in X) \wedge (y \in Y)\})$

$PathG[G] := \exists_P((Ordering[P,V(G)]) \wedge (E(G) = \{\{p_i,p_{i+1}\} \mid i \in \mathbb{N}_1^{|P|-1}\}))$
$CycleG[G] := \exists_C((Ordering[C,V(G)]) \wedge (E(G) = \{\{c_i,c_{i+1}\} \mid i \in \mathbb{N}_1^{|C|-1}\} \cup \{c_n,c_1\}))$
$CompleteG[G] := \forall_{x,y \in V(G)}((x \neq y) \implies \{x,y\} \in E(G))$
$TriangleG[G] := (CompleteG[G]) \wedge (|G| = 3)$

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

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

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

$Isomorphism[\phi,G,H] := (Bijection[\phi,V(G),V(H)]) \wedge (\forall_{x,y \in V(G)}((\{x,y\} \in E(G)) \iff (\{\phi(x),\phi(y)\} \in E(H))))$
$Isomorphic[G,H] := \exists_\phi(Isomorphism[\phi,G,H])$
$IsomorphismEqRel := \forall_{G_1,G_2,G_3}\begin{pmatrix} (G_1 \cong G_1) & \wedge \\ ((G_1 \cong G_2) \implies (G_2 \cong G_1)) & \wedge \\ (((G_1 \cong G_2) \wedge (G_2 \cong G_3)) \implies (G_1 \cong G_3)) \end{pmatrix}$

(1) Bijection and composition properties

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

$PathN[P_n,n] := (PathG[P_n]) \wedge (|P_n| = n)$
$CycleN[C_n,n] := (CycleG[C_n]) \wedge (|C_n| = n)$

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

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

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

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

$CycleLengths[L, G] := L = \{|H| \mid (Subgraph[H, G]) \wedge (CycleG[H])\}$

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

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

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

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

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

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

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

$VCycle[W, G] := (Walk[W, G]) \wedge (w_{|W|} = w_1) \wedge (\forall_{i,j \in \mathbb{N}_2^{|W|-1}}((i \neq j) \implies (w_i \neq w_j)))$

$xyWalk[(x, y), W, G] := (VWalk[W, G]) \wedge (W_1 = x) \wedge (W_{|W|} = y)$

$xyTrail[(x, y), W, G] := (VTrail[W, G]) \wedge (W_1 = x) \wedge (W_{|W|} = y)$

$xyPath[(x, y), W, G] := (VPath[W, G]) \wedge (W_1 = x) \wedge (W_{|W|} = y)$

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

$VClosed[W, G] := (Walk[W, G]) \wedge (w_0 = w_{|W|})$

$VOdd[W, G] := (Walk[W, G]) \wedge (Odd(len(W)))$

$VEven[W, G] := (Walk[W, G]) \wedge (Even(len(W)))$

$PathContainsWalk[P, W, G] := (VPath[P, G]) \wedge (VWalk[W, G]) \wedge \exists_\phi ((OrderedDeletion[\phi, W]) \wedge (P = \phi(W)))$

$xyWalkInxyPath := (xyWalk[(x, y), W, G]) \implies (\exists_P ((xyPath[(x, y), P, G]) \wedge (PathContainsWalk[P, W, G])))$

---

(1) $(l(W) = 0) \implies (P = W)$ ∎ $PathContainsWalk[P, W, G]$

---

(2) $((l(W) > 0) \wedge (\forall_{W'}((l(W') < l(W)) \implies$

$((xyWalk[(x, y), W', G]) \implies (\exists_{P'}((xyPath[(x, y), P', G]) \wedge (PathContainsWalk[P', W', G])))))))) \implies \dots$

   (2.1) If W has no duplicate vertices, then P = W ∎ $PathContainsWalk[P, W, G]$

   (2.2) If W has duplicate vertices, then delete the duplicate vertices and edges between extra copies of unique vertices. This shorter xyWalk
W' has a xyPath P' by IH. ∎ $PathContainsWalk[P', W, G]$

---

(3) $((l(W) > 0) \wedge (\forall_{W'}((l(W') < l(W)) \implies$

$((xyWalk[(x, y), W', G]) \implies (\exists_{P'}((xyPath[(x, y), P', G]) \wedge (PathContainsWalk[P', W', G])))))))) \implies (PathContainsWalk[P, W, G])$

---

(4) By induction: $(xyWalk[(x, y), W, G]) \implies (\exists_P ((xyPath[(x, y), P, G]) \wedge (PathContainsWalk[P, W, G])))$

$ConnectedV[(x, y), G] := \exists_P(xyPath[(x, y), P, G])$

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

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

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

---

(1) By $(xyWalkInxyPath) \wedge (xyPath[(x, y), W, G]) \iff (xyPath[(y, x), W, G])$

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

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

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

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

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

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

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

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

(1)	Starting from $E(G) = \emptyset$, $|mathcal H| = n$
(2)	Adding an edge would decrease the number of components by 0 or 1, so after adding k edges, $n - k \leq |mathcal H|$

$RemoveV[G - W, W, G] := (V(G - W) = V(G) \setminus W) \wedge (E(G - W) = \{\{x, y\} \in E(G) \mid x, y \in V(G - W)\})$
$RemoveE[G - E, E, G] := (V(G - E) = V(G)) \wedge (E(G - E) = E(G) \setminus E)$
$AddE[G + e, e, G] := (e \in V(G)^{\{2\}}) \wedge (V(G + e) = V(G)) \wedge (E(G + e) = E(G) \cup \{e\})$
$InducedSubgraph[G[T], T, G] := G[T] = G - \bar{T}$
$SpanningSubgraph[H, G] := (Subgraph[H, G]) \wedge (V(H) = V(G))$

$CutVertex[v, G] := (NumComponents[c_1, G]) \wedge (NumComponents[c_2, G - v]) \wedge (c_2 > c_1)$
$CutEdge[e, G] := (NumComponents[c_1, G]) \wedge (NumComponents[c_2, G - e]) \wedge (c_2 > c_1)$
$CutEdgeEquiv := (CutEdge[e, G]) \iff (\neg\exists_C((Subgraph[C, G]) \wedge (CycleG[C]) \wedge (e \in E(C))))$

(1)	Let $(Component[H, G]) \wedge (e = \{x, y\} \in E(H))$
(2)	$(CutEdge[e, G]) \iff (CutEdge[e, H]) \iff (\neg Connected[H - e])$
(3)	WTS: $(Connected[H - e]) \iff (\exists_C(((CycleG[C]) \wedge Subgraph[C, G]) \wedge (e \in E(C))))$
(4)	$(Connected[H - e]) \implies \ldots$
(4.1)	$\exists_P((PathG[P]) \wedge (Subgraph[P, H - e]))$ ▮ $P + e$ must contain a cycle ▮ $\exists_C(((CycleG[C]) \wedge Subgraph[C, G]) \wedge (e \in E(C)))$
(5)	$(Connected[H - e]) \implies (\exists_C(((CycleG[C]) \wedge Subgraph[C, G]) \wedge (e \in E(C))))$
(6)	$(\exists_C(((CycleG[C]) \wedge Subgraph[C, G]) \wedge (e \in E(C)))) \implies \ldots$
(6.1)	$Component[H, G]$ ▮ $Connected[H]$
(6.2)	$(u, v \in V(H)) \implies \ldots$
(6.2.1)	$\exists_P(xyPath[(u, v), P, H])$
(6.2.2)	$(e \notin E(P)) \implies (\exists_P(xyPath[(u, v), P, H]))$
(6.2.3)	$(e \in E(P)) \implies \ldots$
(6.2.3.1)	$P' = u - xPath + x - yCycleG + y - vPath$
(6.2.3.2)	$xyPath[(u, v), P', H - e]$ ▮ $\exists_P(xyPath[(u, v), P, H])$
(6.2.4)	$(e \in E(P)) \implies (\exists_P(xyPath[(u, v), P, H]))$
(6.2.5)	$\exists_P(xyPath[(u, v), P, H])$
(6.3)	$(u, v \in V(H)) \implies (\exists_P(xyPath[(u, v), P, H - e]))$ ▮ $Connected[H - e]$
(7)	$(\exists_C(((CycleG[C]) \wedge Subgraph[C, G]) \wedge (e \in E(C)))) \implies (Connected[H - e])$

$OddCycleInClosedOddWalk := ((VClosed[W, G]) \wedge (VOdd[W, G])) \implies (\exists_C((VCycle[C, G]) \wedge (VOdd[C, G]) \wedge (CycleInWalk[C, W, G]))$

(1)	$(len(W) = 1) \implies (W = C)$ ▮ $\exists_C((VCycle[C, G]) \wedge (VOdd[C, G]) \wedge (CycleInWalk[C, W, G]))$
(2)	$((len(W) > 1) \wedge (\forall_{W'}((len(W') < len(W)) \implies$ $(((VClosed[W', G]) \wedge (VOdd[W', G])) \implies (\exists_{C'}((VCycle[C', G]) \wedge (VOdd[C', G]) \wedge (CycleInWalk[C', W', G])))))))) \implies \ldots$
(2.1)	If W has no repeated vertex other than the first and last, then $C = W$ ▮ $\exists_C((VCycle[C, G]) \wedge (VOdd[C, G]) \wedge (CycleInWalk[C, W, G]))$
(2.2)	If W has a repeated vertex v, then break W into two v Walks W_1, W_2. Since W is odd, W_1, W_2 are odd and even walks (not necessarily respectively).
(2.3)	WLOG let W_1 be the smaller odd walk, then by IH $\exists_{C'}((VCycle[C', G]) \wedge (VOdd[C', G]) \wedge (CycleInWalk[C', W_1, G]))$
(2.4)	$\exists_C((VCycle[C, G]) \wedge (VOdd[C, G]) \wedge (CycleInWalk[C, W, G]))$
(3)	$((len(W) > 1) \wedge (\forall_{W'}((len(W') < len(W)) \implies$ $(((VClosed[W', G]) \wedge (VOdd[W', G])) \implies (\exists_{C'}((VCycle[C', G]) \wedge (VOdd[C', G]) \wedge (CycleInWalk[C', W', G])))))))) \implies$ $\exists_C((VCycle[C, G]) \wedge (VOdd[C, G]) \wedge (CycleInWalk[C, W, G])$
(4)	By induction: $\exists_C((VCycle[C, G]) \wedge (VOdd[C, G]) \wedge (CycleInWalk[C, W, G]))$

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

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

(1)	$(Bipartite[G]) \implies \ldots$
(1.1)	Every step alternates between each bipartition. Thus the end vertex of the odd walk cannot be the start vertex, and it is not a cycle.
(1.2)	$\neg\exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (VOdd[C, G]))$
(2)	$(Bipartite[G]) \implies (\neg\exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (VOdd[C, G])))$
(3)	$(\neg\exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (VOdd[C, G]))) \implies \ldots$

(3.1)	Consider each nontrivial component H, and pick a $u \in V(H)$.
(3.2)	Let $X = \{v \in H \mid Even(d(v, u))\}$ and let $Y = \{v \in H \mid Odd(d(v, u))\}$.
(3.3)	Suppose X or Y are not independent sets. WLOG choose X.
(3.3.1)	X must contain an edge - call it $\{v, v'\}$
(3.3.2)	A closed odd walk could be: min u-v path (+ even) and v-v' (+ 1) and min v'-u path (+ even)
(3.3.3)	By $OddCycleInClosedOddWalk$, there exists an odd cycle in G. ▌ ⊥
(3.4)	X and Y are independent sets; futhermore X, Y are bipartitions of G. ▌ $Bipartite[G]$
(4)	$(\neg \exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (VOdd[C, G]))) \implies (Bipartite[G])$
(5)	$(Bipartite[G]) \iff (\neg \exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (VOdd[C, G])))$

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

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

(1)	$(k = 1) \implies \dots$
(1.1)	$(\exists_{\mathcal{B}}((|\mathcal{B}| = k) \wedge (\forall_{B \in \mathcal{B}}(BipartiteG[B])) \wedge (UnionG[K_n, \mathcal{B}]))) \iff (Bipartite[K_n])$
(1.2)	$(n \leq 2^k) \implies \dots$
(1.2.1)	$n \leq 2^1 = 2$ ▌ $((n = 1) \vee (n = 2))$
(1.2.2)	$(BipartiteG[K_1]) \wedge (BipartiteG[K_2])$ ▌ $Bipartite[K_n]$
(1.3)	$(n \leq 2^k) \implies (Bipartite[K_n])$
(1.4)	$(Bipartite[K_n]) \implies \dots$
(1.4.1)	$(n > 2) \implies \dots$
(1.4.1.1)	K_n has an odd cycle
(1.4.1.2)	$BipartiteEquiv$ and K_n has an odd cycle ▌ $\neg Bipartite[K_n]$ ▌ ⊥
(1.4.2)	$(n > 2) \implies (\bot)$ ▌ $n \leq 2$
(1.5)	$(Bipartite[K_n]) \implies (n \leq 2)$
(1.6)	$(Bipartite[K_n]) \iff (n \leq 2)$ ▌ $(\exists_{\mathcal{B}}((|\mathcal{B}| = k) \wedge (\forall_{B \in \mathcal{B}}(BipartiteG[B])) \wedge (UnionG[K_n, \mathcal{B}]))) \iff (n \leq 2)$
(2)	$(k = 1) \implies ((\exists_{\mathcal{B}}((|\mathcal{B}| = k) \wedge (\forall_{B \in \mathcal{B}}(BipartiteG[B])) \wedge (UnionG[K_n, \mathcal{B}]))) \iff (n \leq 2))$
(3)	$((k > 1) \wedge (\forall_{k'}((k' < k) \implies ((\exists_{\mathcal{B}}((|\mathcal{B}| = k') \wedge (\forall_{B \in \mathcal{B}}(BipartiteG[B])) \wedge (UnionG[K_n, \mathcal{B}]))) \iff (n \leq 2^{k'}))))) \implies \dots$
(3.1)	THE SUBGRAPH INDUCED BY X AND Y ARE NECESSARILY COMPLETE!!!!!!!!!!!!
(4)	$((k > 1) \wedge (\forall_{k'}((k' < k) \implies ((\exists_{\mathcal{B}}((|\mathcal{B}| = k') \wedge (\forall_{B \in \mathcal{B}}(BipartiteG[B])) \wedge (UnionG[K_n, \mathcal{B}]))) \iff (n \leq 2^{k'}))))) \implies 123123$

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

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

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

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

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

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

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

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

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

$Order[|G|,G] := |G| = |V(G)|$

$Size[e(G),G] := e(G) = |E(G)|$

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

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

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

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

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

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

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

---

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

$CompleteG[K_n,n] := (|K_n| = n) \wedge (e(K_n) = \binom{n}{2})$

$EmptyG[E_n,n] := (|K_n| = n) \wedge (e(K_n) = 0)$

$TrivialG[G] := G = K_1 = E_1$

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

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

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

$Degree[d(x),x,G] := d(x) = |\Gamma_G(x)|$

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

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

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

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

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

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

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

---

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

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

---

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

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

---

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

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

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

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

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

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

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

$ClosedWalk[W,G] := (Walk[W,G]) \wedge (w_{|W|} = w_1)$
$Circuit[W,G] := (Trail[W,G]) \wedge (ClosedWalk[W,G])$
$CycleW[W,G] := (ClosedWalk[W,G]) \wedge (\forall_{i \in \mathbb{N}_2^{|W|-1}}(w_0 \neq w_i \neq w_{|W|})) \wedge (\forall_{i,j \in \mathbb{N}_2^{|W|-1}}((i \neq j) \implies (w_i \neq w_j))) \wedge (|W| - 1 \geq 3)$

$CycleE[E,(W,G)] := (CycleW[W,G]) \wedge (E = \{\{w_i, w_{i+1}\} \mid i \in \mathbb{N}_1^{|W|-1}\})$
$EvenCycleW[W,G] := (CycleW[W,G]) \wedge (Even(|W| - 1))$
$OddCycleW[W,G] := (CycleW[W,G]) \wedge (Odd(|W| - 1))$
$TriangleW[W,G] := (CycleW[W,G]) \wedge (|W| - 1 = 3)$

$IndependentV[V,G] := \forall_{x,y \in V}(\neg AdjacentV[(x,y),G])$
$IndependentE[E,G] := \forall_{a,b \in E}(\neg AdjacentE[(a,b),G])$
$IndependentPathG[\mathcal{P},G] := \exists_{x,y \in V(G)}\forall_{P,Q \in \mathcal{P}}((P \neq Q) \implies (V(P) \cap V(Q) = \{x,y\}))$
$IndependentVEquiv := IndependentV \iff (SubgraphInducedByV[] \cong E_n)$

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

$CycleG[P,V] := (V(P) = V) \wedge (E(P) = \{\{v_i, v_{i+1}\} \mid i \in \mathbb{N}_1^{|V|-1}\} \cup \{v_{|V|}, v_1\})$
$PathInG[P,V,G] := (PathG[P,V]) \wedge (Subgraph[P,G])$
$PathXY[P,(x,y),V,G] := (PathInG[P,V,G]) \wedge ((v_1, v_{|V|}) = (x,y))$
$CycleInG[C,V,G] := (CycleG[C,V]) \wedge (Subgraph[C,G])$

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

(1)	$(\exists_C((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E,(C,G)])\}) \wedge (Partition[\mathcal{E}, E(G)]))) \implies \dots$
(1.1)	$\forall_{v \in V(G)}(d(v) = 2 * |\{v \mid (C \in \mathcal{C}) \wedge (v \in C)\}|)$ ▌ $\forall_{v \in V(G)}(Even(d(v)))$
(2)	$(\exists_C((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E,(C,G)])\}) \wedge (Partition[\mathcal{E}, E(G)]))) \implies (\forall_{v \in V(G)}(Even(d(v))))$
(3)	$(\forall_{v \in V(G)}(Even(d(v)))) \implies \dots$
(3.1)	$(e(G) = 0) \implies (\exists_C((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E,(C,G)])\}) \wedge (Partition[\mathcal{E}, E(G)])))$
(3.2)	$(e(G) \neq 0) \implies \dots$
(3.2.1)	$(e(G) > 0) \wedge (\forall_{v \in V(G)}(Even(d(v))))$ ▌ $\exists_{x_0 \in V(G)}(d(x_0) \geq 2)$
(3.2.2)	There exists a Path P of maximal length with endvertices (x_0, x_l).
(3.2.3)	$(d(x_0) \geq 2)$ ▌ Let y be another vertex adjacent to x_0 that is not x_1.
(3.2.4)	If y is not in P, then P is not a maximal Path - contradiction.
(3.2.5)	Thus y is in P, and P contains a cycle C.
(3.2.6)	Let $G' = G - E(C)$. ▌ $(\forall_{v \in V(G')}(Even(d_{G'}(v))))$ ▌ Repeat on G' until all disjoint cycles $\mathcal{C}$ are found.
(3.2.7)	$\exists_C((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E,(C,G)])\}) \wedge (Partition[\mathcal{E}, E(G)]))$
(3.3)	$(e(G) \neq 0) \implies (\exists_C((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E,(C,G)])\}) \wedge (Partition[\mathcal{E}, E(G)])))$
(3.4)	$\exists_C((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E,(C,G)])\}) \wedge (Partition[\mathcal{E}, E(G)]))$
(4)	$(\forall_{v \in V(G)}(Even(d(v)))) \implies (\exists_C((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E,(C,G)])\}) \wedge (Partition[\mathcal{E}, E(G)])))$
(5)	$(\forall_{v \in V(G)}(Even(d(v)))) \iff (\exists_C((\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge (CycleE[C_E,(C,G)])\}) \wedge (Partition[\mathcal{E}, E(G)])))$

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

(1)	$(\neg \exists_W(Triangle[W,G])) \implies \dots$
(1.1)	$\neg \exists_W(Triangle[W,G])$ ▌ $\forall_{\{x,y\} \in E(G)}(\Gamma(x) \cap \Gamma(y) = \emptyset)$ ▌ $\forall_{\{x,y\} \in E(G)}(d(x) + d(y) \leq n)$
(1.2)	$\sum_{\{x,y\} \in E(G)} (d(x) + d(y)) \leq n(e(G))$
(1.3)	$\sum_{\{x,y\} \in E(G)} (d(x) + d(y)) = \sum_{v \in V(G)} ((d(v))^2)$
(1.4)	$\sum_{v \in V(G)} ((d(v))^2) \leq n(e(G))$ ▌ $n \sum_{v \in V(G)} ((d(v))^2) \leq n^2(e(G))$
(1.5)	$(SumDegrees) \wedge (CauchysInequality)$ ▌ $(2e(G))^2 = (\sum_{v \in V(G)} (d(v)))^2 \leq \sum_{v \in V(G)} (d(v))^2$
(1.6)	$(2e(G))^2 \leq n^2(e(G))$ ▌ $e(G) \leq n^2/4$
(1.7)	$(e(G) > \lfloor n^2/4 \rfloor) \wedge (e(G) \leq n^2/4)$ ▌ $\bot$

(2) $(\neg \exists_W (Triangle[W, G])) \implies (\bot)$ ▮ $\exists_W (Triangle[W, G])$

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

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

---

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

(2) By cases:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[Notation] $(K(n_1, ..., n_r)) := CompleteRpartiteG$

[Notation] $(K_r(t)) := K(t, ..., t)$

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

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

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

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

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

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

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

---

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

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

---

(1) SumDeg

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

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

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

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

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

(1)   TODO $\phi = \dots$

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

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

$GraphCartesian[G_1 \times G_2, G_1, G_2] := \begin{pmatrix} (V = V(G_1) \times V(G_2)) & \wedge \\ (E = \{((x_1, y_1), (x_2, y_2)) \mid ((x_1 = x_2) \wedge (\{y_1, y_2\} \in E(G_2))) \vee ((y_1 = y_2) \wedge (\{x_1, x_2\} \in E(G_1)))\}) \wedge \\ (G_1 \times G_2 = (V, E)) \end{pmatrix}$

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

$GraphConjunction[G_1 \wedge G_2, G_1, G_2] := \begin{pmatrix} (V = V(G_1) \times V(G_2)) & \wedge \\ (E = \{((x_1, y_1), (x_2, y_2)) \mid (\{x_1, x_2\} \in E(G_1)) \wedge (\{y_1, y_2\} \in E(G_2))\}) \wedge \\ (G_1 \wedge G_2 = (V, E)) \end{pmatrix}$

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

$KroneckerProperties := \dots$

(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

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

forest -> decomponents into trees

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

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

(1)   TODO

Chapter 2

Abstract Algebra

2.1 Functions

$Rel[r, X] := (X \neq \emptyset) \wedge (r \subseteq X)$
$Func[f, X, Y] := (Rel[f, X \times Y]) \wedge (\forall_{x \in X} \exists!_{y \in Y}(\langle x, y \rangle \in f))$
$Comp[g \circ f, f, g, X, Y, Z] := (Func[f, X, Y]) \wedge (Func[g, Y, Z]) \wedge (g \circ f = \{\langle x, g(f(x)) \rangle \in X \times Z \mid x \in X\})$

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

(1) TODO

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

(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, Paritions

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

(1) TODO

$Divides[a, b] := (a, b \in \mathbb{Z}) \wedge (\exists_{c \in \mathbb{Z}}(b = ac))$
$ComDiv[a, b, c] := (Divides[a, b]) \wedge (Divides[a, c])$
$GCD[a, b, c] := (ComDiv[a, b, c]) \wedge (\forall_{d \in \mathbb{Z}}(((Divides[d, b]) \wedge (Divides[d, c])) \implies (Divides[d, a])))$
$RelPrime[a, b] := GCD[1, a, b]$
$CongRel[a, b, n] := Divides[n, a - b]$

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

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

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

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

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

(1)	TODO : $Partition[EqClass_1, EqClass_2, ...]$

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

(1)	TODO

2.3   Groups

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

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

(1)	$(a * b = a * c) \implies ...$
(1.1)	$a \in G$ ▐ $\exists_{a^{-1} \in G}(a * a^{-1} = e = a^{-1} * a)$
(1.2)	$Function[*, G, G]$ ▐ $a^{-1} * a * b = a^{-1} * a * c$
(1.3)	$(\forall_{a,b,c \in G}((a * b) * c = a * (b * c))) \wedge (\forall_{a \in G}\exists_{a^{-1} \in G}(a * a^{-1} = e = a^{-1} * a))$ ▐ $b = c$
(2)	$(a * b = a * c) \implies (b = c)$
(3)	$(a * c = b * c) \implies ...$
(3.1)	TODO
(4)	$(a * c = b * c) \implies (a = b)$
(5)	$((a * b = a * c) \implies (b = c)) \wedge ((a * c = b * c) \implies (a = b))$

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

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

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

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

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

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

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

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

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

2.4 Subgroups

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

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

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

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

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

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

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

  (2.2) $\emptyset \neq H$ ▮ $\exists_h(h \in H)$

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

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

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

  (2.6) $Group[H, *]$

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

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

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

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

(1) TODO

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

(1) $Group[G, *]$

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

(3) $(H_1 \subseteq G) \wedge (H_2 \subseteq G)$ ▮ $H_1 \cap H_2 \subseteq G$

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

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

  (5.1) $a, b \in H_1$ ▮ $a * b \in H_1$

  (5.2) $a, b \in H_2$ ▮ $a * b \in H_2$

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

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

(7) $(a \in H_1 \cap H_2) \implies \ldots$

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

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

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

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

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

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

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

(2) $C(g) \subseteq G$ ▮ $\emptyset \neq C(g) \subseteq G$

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

(3.1)	$(a * g = g * a) \wedge (b * g = g * b)$

(3.2)	$(a * b) * g = a * (b * g) = a * (g * b) = a * (g * a) * b = (g * a) * b = g * (a * b)$ ▌ $a * b \in C(g)$

(4)	$(a, b \in C(g)) \implies (a * b \in C(g))$ ▌ $\forall_{a,b \in C(g)}(a * b \in C(g))$

(5)	$(a \in C(g)) \implies \dots$

(5.1)	$a * g = g * a$

(5.2)	$a^{-1} * (a * g) * a^{-1} = a^{-1} * (g * a) * a^{-1}$ ▌ $g * a^{-1} = a^{-1} * g$ ▌ $a^{-1} \in C(g)$

(6)	$(a \in C(g)) \implies (a^{-1} \in C(g))$ ▌ $\forall_{a \in C(g)}(a^{-1} \in C(g))$

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

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

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

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

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)	$H \subseteq G$ ▌ $\exists_{m \in \mathbb{Z}^+}((g^m \in H) \wedge (\forall_{k \in \mathbb{Z}^+}((k < m) \implies (g^k \notin H))))$

(3)	$(b \in H) \implies \dots$

(3.1)	$H \subseteq G$ ▌ $\exists_{n \in \mathbb{Z}^+}(b = g^n)$

(3.2)	$(DivisionAlgorithm) \wedge (n \in \mathbb{Z}) \wedge (m \in \mathbb{Z}^+)$ ▌ $\exists!_{q,r \in \mathbb{Z}}((n = mq + r) \wedge (0 \leq r < m))$

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

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

(3.5)	$(g^r \in H) \wedge (0 \leq r < m) \wedge (\forall_{k \in \mathbb{Z}^+}((k < m) \implies (g^k \notin H)))$ ▌ $r = 0$

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

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

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

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

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

(5.3)	$Induction$ ▌ $b = (g^m)^k \in H$ ▌ $b \in H$

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

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

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

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

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

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

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

2.5.2 Symmetric and Alternating Groups

$SymmetricGroup[S_n, n] := S_n = \{\text{permutation of a set with n elements}\}$
$SymmetricGroupOrder := o(S_n) = n!$
$SymmetricGroupAsDisjoinsCycles := \forall_{\sigma \in S_n} \exists_{\Sigma \subseteq S_n}((DisjointCycles[\Sigma]) \wedge (\sigma = \prod(\sigma_i)))$
$SymmetricGroupAsTranspositions := \forall_{\sigma \in S_n} \exists_{\Sigma \subseteq S_n}((Transpositions[\Sigma]) \wedge (\sigma = \prod(\sigma_i)))$

$vFunction[v(\sigma), \sigma, S_n] := v(\sigma) = n - |DisjointFullCycles[\Sigma]|$
$signFunction[sign(\sigma), \sigma, S_n] := sign(\sigma) = (-1)^{v(\sigma)}$
$EvenPermutation[\sigma, S_n] := sign(\sigma) = 1$
$OddPermutation[\sigma, S_n] := sign(\sigma) = -1$

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

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

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

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

(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)	$((a \sim b) \wedge (b \sim c)) \implies (a * b^{-1}, b * c^{-1} \in H) \implies (a * c^{-1} = (a * b^{-1}) * (b * c^{-1}) \in H)$ ▮ $a \sim c$
(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)	$(CosetInduceEqRel) \wedge (EqRelInducesPartition) \wedge (CosetCardinality)$ ▮ $(o(G) = o(H)|G : H|) \wedge (Divides[o(H), o(G)])$

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

(1)	$CyclicSubgroup[<g>, g, G, *]$ ▮ $Order[<g>] = m$
(2)	$(LagrangeTheorem) \wedge (CyclicSubgroup)$ ▮ $Divides[Order[<g>], Order[G]]$ ▮ $Divides[m, n]$
(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 |

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

| (1) | $(LagrangeTheorem) \land (SubgroupIntersection) \land (RelPrime(o(H), o(K)))$ ▌ $H \cap K = \{e\}$ |

2.7   Homomorphisms

$Homomorphism[\phi, G, *, H, \diamond] := (Function[\phi, G, H]) \land (\forall_{a,b \in G}(\phi(a * b) = \phi(a) \diamond \phi(b)))$
$Monomorphism[\phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \land (Inj[\phi, G, H])$
$Epimorphism[\phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \land (Surj[\phi, G, H])$
$Isomorphism[\phi, G, *, H, \diamond] := (Homomorphism[\phi, G, *, H, \diamond]) \land (Bij[\phi, G, H])$
$Isomorphic[G, *, H, \diamond] := \exists_{\phi}(Isomorphism[\phi, G, *, H, \diamond])$ ** Notation: $G \cong H$ **
$Automorphism[\phi, G, *] := Isomorphism[\phi, G, *, G, *]$

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

| (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) | $e_H = \phi(e_G)^{-1} \diamond \phi(e_G) = \phi(e_G)^{-1} \diamond (\phi(e_G) \diamond \phi(e_G)) = \phi(e_G)$ ▌ $e_H = \phi(e_G)$ |

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

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

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

(1)	$(n = 1) \implies \dots$
(1.1)	$\phi(g^n) = \phi(g) = \phi(g)^n$ ▌ $\phi(g^n) = \phi(g)^n$
(2)	$(n = 1) \implies (\phi(g^n) = \phi(g)^n)$
(3)	$(\forall_{m \in \mathbb{N}^+}((m \le n) \implies (\phi(g^m) = \phi(g)^m))) \implies \dots$
(3.1)	$\phi(g^{n+1}) = \phi(g^n * g) = \phi(g)^n \diamond \phi(g) = \phi(g)^{n+1}$ ▌ $\phi(g^{n+1}) = \phi(g)^{n+1}$
(4)	$(\forall_{m \in \mathbb{N}^+}((m \le n) \implies (\phi(g^m) = \phi(g)^m))) \implies (\phi(g^{n+1}) = \phi(g)^{n+1})$
(5)	$((n = 1) \implies (\phi(g^n) = \phi(g)^n)) \land ((\forall_{m \in \mathbb{N}^+}((m \le n) \implies (\phi(g^m) = \phi(g)^m))) \implies (\phi(g^{n+1}) = \phi(g)^{n+1}))$ $\dots$
(6)	$\dots \forall_{n \in \mathbb{N}^+}(\phi(g^n) = \phi(g)^n)$

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

(1)	$OrderElDivOrder$ ▌ $g^n = e_G$
(2)	$(IdMapsId) \land (ExpMapsExp)$ ▌ $e_H = \phi(e_G) = \phi(g^n) = \phi(g)^n$ ▌ $\phi(g)^n = e_H$
(3)	$(ExpModOrderCorollary) \land (OrderEl[m, \phi(g), H, \diamond]) \land (\phi(g)^n = e_H)$ ▌ $Divides[m, n]$

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

(1)	$Inj[\phi, G, H]$ ▌ $\forall_{g_1,g_2 \in G}((\phi(g_1) = \phi(g_2)) \implies (g_1 = g_2))$
(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)	$(\forall_{g_1,g_2 \in G}((\phi(g_1) = \phi(g_2)) \implies (g_1 = g_2))) \land (e_H = \phi(g^m)) \land (e_H = \phi(g^n))$ ▌ $g^m = g^n$
(5)	$(OrderEl[m, \phi(g), H, \diamond]) \land (Order[n, G, *]) \land (g^m = g^n)$ ▌ $m = n$

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

| (1) | $FuncComp$ ▌ $Func[\theta \circ \phi, G, K]$ |
| (2) | $(g_1, g_2 \in G) \implies \dots$ |

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

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

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

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

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

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

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

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

(2) $im_\phi \subseteq H$ ▮ $\emptyset \neq im_\phi \subseteq H$

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

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

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

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

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

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

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

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

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

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

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

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

(1) $CyclicGroup[G, *]$ ▮ $\exists_{r \in G}(Generator[r, G, *])$ ▮ $G = <r> = \{r^n \mid n \in \mathbb{Z}\}$

(2) $ExpMapsExp$ ▮ $im_\phi = \{\phi(g) \mid g \in G\} = \{\phi(r^n) \mid n \in \mathbb{Z}\} = \{\phi(r)^n \mid n \in \mathbb{Z}\} = <\phi(r)>$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(2) $\mathcal{G} = \{[g] \mid g \in G\}$ ▌ $(Partition[\mathcal{G}, G]) \wedge (|\mathcal{G}| = |im_\phi|)$

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

(4) $Partition[\mathcal{G}, G]$ ▌ $|G| = |\mathcal{G}||ker_\phi| = |im_\phi||ker_\phi|$

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

(1) $KerImPartitionsG$ ▌ ▌ $|G| = |ker_\phi||im_\phi|$ ▌ $Divides[|im_\phi|, |G|]$

(2) $(LagrangeTheorem) \wedge (ImageSubgroupCodomain)$ ▌ $|H| = |im_\phi||H : im_\phi|$ $Divides[|im_\phi|, |H|]$

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) $(a, b, c \in G) \implies \ldots$

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

  (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) $((a \sim^* b) \wedge (b \sim^* c)) \implies ((b = x_b^{-1} * a * x_b) \wedge (c = x_c^{-1} * b * x_c)) \implies \ldots$

  (1.4) $\ldots (c = x_c^{-1} * x_b^{-1} * a * x_b * x_c = (x_b * x_c)^{-1} * a * (x_b * x_c))$ ▌ $a \sim^* c$

(2) $EqRel[\sim^*, G]$

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

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

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

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

(1) $(C_g = \{g\}) \implies \ldots$

  (1.1) $(x \in G) \implies \ldots$

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

    (1.1.2) $(C_g = \{g\}) \wedge (x^{-1}gx \in C_g)$ ▌ $x^{-1}gx = g$ ▌ $gx = xg$

  (1.2) $(x \in G) \implies (gx = xg)$ ▌ $\forall_{x \in G}(gx = xg)$ ▌ $g \in Z(G)$

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

(3) $(g \in Z(G)) \implies \ldots$

  (3.1) $(g \in Z(G)) \wedge (Group[G, *])$ ▌ $(\forall_{c \in G}(gc = cg)) \wedge (\exists_e(e \in G))$

  (3.2) $(x \in G) \implies \ldots$

    (3.2.1) $(\forall_{c \in G}(gc = cg)) \wedge (\exists_e(e \in G))$ ▌ $(\exists_{c \in G}(x = c^{-1}gc)) \iff (\exists_{c \in G}(x = c^{-1}gc = c^{-1}cg = g)) \iff (x = g) \iff (x \in \{g\})$

  (3.3) $(x \in G) \implies ((\exists_{c \in G}(x = c^{-1}gc)) \iff (x \in \{g\}))$ ▌ $\forall_{x \in G}((x \in \{g\}) \iff (\exists_{c \in G}(x = c^{-1}gc)))$

  (3.4) $(ConjugacyClassEquiv) \wedge (\forall_{x \in G}((x \in \{g\}) \iff (\exists_{c \in G}(x = c^{-1}gc))))$ ▌ $C_g = \{g\}$

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

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

(1) $(n = 1) \implies \ldots$

  (1.1) $(x^{-1}gx)^n = (x^{-1}gx)^1 = x^{-1}g^1x = x^{-1}g^nx$ ▌ $(x^{-1}gx)^n = x^{-1}g^nx$

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

(3) $((n > 1) \land (\forall_{m \in \mathbb{N}^+}((m \le n) \implies ((x^{-1}gx)^m = x^{-1}g^mx)))) \implies \dots$

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

(4) $((n > 1) \land (\forall_{m \in \mathbb{N}^+}((m \le n) \implies ((x^{-1}gx)^m = x^{-1}g^mx)))) \implies ((x^{-1}gx)^{n+1} = x^{-1}g^{n+1}x)$

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

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

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

(2) $ConjugateExp$ ▮ $e = g_2{}^{o(g_2)} = (c^{-1}g_1c)^{o(g_2)} = c^{-1}g_1{}^{o(g_2)}c$ ▮ $e = c^{-1}g_1{}^{o(g_2)}c$ ▮ $g_1{}^{o(g_2)} = e$

(3) $ExpModOrderCorollary$ ▮ $Divides[o(g_2), o(g_1)]$

(4) $ConjugateExp$ ▮ $e = g_1{}^{o(g_1)} = (cg_2c^{-1})^{o(g_1)} = cg_2{}^{o(g_1)}c^{-1}$ ▮ $e = cg_2{}^{o(g_1)}c^{-1}$ ▮ $g_2{}^{o(g_1)} = e$

(5) $ExpModOrderCorollary$ ▮ $Divides[o(g_1), o(g_2)]$

(6) $(Divides[o(g_2), o(g_1)]) \land (Divides[o(g_1), o(g_2)]) \land (g_1, g_2 \in \mathbb{N}^+)$ ▮ $o(g_1) = o(g_2)$

(7) ==

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

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

 (9.1) $e \ne g_2{}^m = (c^{-1}g_1c)^m = c^{-1}g_1{}^mc$ ▮ $e \ne c^{-1}g_1{}^mc$ ▮ $e = c * e * c^{-1} \ne g_1{}^m$ ▮ $g_1{}^m \ne e$

(10) $(m < o(g_2)) \implies (e \ne g_1{}^m)$ ▮ $\forall_{m \in \mathbb{Z}^+}((m < o(g_2)) \implies (g_1{}^m \ne e))$

(11) $(g_1{}^{o(g_2)} = e) \land (\forall_{m \in \mathbb{Z}^+}((m < o(g_2)) \implies (g_1{}^m \ne e)))$ ▮ $o(g_1) = o(g_2)$

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

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

 (1.1) $a \in C(g)$ ▮ $ag = ga$

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

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

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

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

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

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

(5) $(c^{-1}C(g)c \subseteq C(h)) \land (C(h) \subseteq c^{-1}C(g)c)$ ▮ $C(h) = c^{-1}C(g)c$

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

(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) $\dots (Func[\phi, C_g, G : C(g)]) \land (Inj[\phi, C_g, G : C(g)]) \land (Surj[\phi, C_g, G : C(g)])$ ▮ $Bij[\phi, C_g, G : C(g)]$

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

(6) $(LagrangeTheorem) \land (SubgroupCenter) \land (|C_g| = |G : C(g)|)$ ▮ $o(G) = o(C(g))|G : C(g)|$ ▮ $o(G) = o(C(g))|C_g|$

2.10   Normal Subgroups

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

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

(1) $SubgroupCenter$ ▮ $Subgroup[Z(G), G, *]$

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

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

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

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

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

(1) $(NormalSubgroup[H, G, *]) \implies \ldots$

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

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

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

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

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

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

  (1.5) $(b \in H) \implies (b \in C_b \subseteq \bigcup_{z \in H}(C_z))$ ▌ $(b \in H) \implies (b \in \bigcup_{z \in H}(C_z))$

  (1.6) $(b \notin H) \implies (\forall_{a \in H}(b \notin C_a)) \implies (b \notin \bigcup_{z \in H}(C_z))$ ▌ $(b \notin H) \implies (b \notin \bigcup_{z \in H}(C_z))$

  (1.7) $((b \in H) \implies (b \in \bigcup_{z \in H}(C_z))) \wedge ((b \notin H) \implies (b \notin \bigcup_{z \in H}(C_z)))$ ▌ $(b \in H) \iff (b \in \bigcup_{z \in H}(C_z))$

  (1.8) $\forall_b((b \in H) \iff (b \in \bigcup_{z \in H}(C_z)))$ ▌ $H = \bigcup_{z \in H}(C_z)$

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

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

(1) $CosetCardinality$ ▌ $\forall_{g \in G}(|Hg| = |gH|)$ ▌ $(\forall_{g \in G}((Hg \subseteq gH) \iff (Hg = gH)))$

(2) $(\forall_{g \in G}((Hg \subseteq gH) \iff (Hg = gH)))$ ▌ $(NormalSubgroup[H, G, *]) \iff (\forall_{h \in H} \forall_{g \in G}(g^{-1}hg \in H)) \iff \ldots$

(3) $\ldots (\forall_{h \in H} \forall_{g \in G}(hg \in gH)) \iff (\forall_{g \in G}(Hg \subseteq gH)) \iff (\forall_{g \in G}(Hg = gH))$

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

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

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

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

(2) $((h \in ker_\phi) \wedge (g \in G)) \implies \ldots$

  (2.1) $h \in ker_\phi$ ▌ $\phi(h) = e_H$

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

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

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

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

2.11   Quotient Groups

$QuotientSet[G/H, H, G, *] := (Subgroup[H, G, *]) \wedge (G/H = \{Hg \mid g \in G\})$
$CosetMul[\bar{*}, H, G, *] := (Subgroup[H, G, *]) \wedge (\forall_{Hx, Hy \in G/H}(Hx \bar{*} Hy = \{h_1xh_2y \mid h_1, h_2 \in H\}))$
$SubsetMul[\bar{\times}, G, *] := (Group[G, *]) \wedge (\forall_{A, B \subseteq G}(A \bar{\times} B = \{a * b \mid (a \in A) \wedge (b \in B)\}))$

$QuotientGroupLemma := ((NormalSubgroup[H, G, *]) \wedge (x, y, z \in G)) \implies ((\exists_{h_1, h_2 \in H}(z = h_1xh_2y)) \iff (\exists_{h_3 \in H}(z = h_3xy)))$

(1) $(\exists_{h_1, h_2 \in H}(z = h_1xh_2y)) \implies \ldots$

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

(1.2) $(NormalSubgroup[H,G,*]) \wedge (x^{-1} \in G) \wedge (h_2 \in H)$ ▌ $(x^{-1})^{-1}h_2x^{-1} = xh_2x^{-1} \in H$

(1.3) $(Group[H,*]) \wedge (h_1, xh_2x^{-1} \in H)$ ▌ $h_1xh_2x^{-1} \in H$

(1.4) $(h_1xh_2x^{-1})(xy) = h_1xh_2y = z$ ▌ $(h_1xh_2x^{-1})(xy) = z$

(1.5) $(h_1xh_2x^{-1} \in H) \wedge ((h_1xh_2x^{-1})(xy) = z)$ ▌ $\exists_{h_3 \in H}(z = h_3xy)$

(2) $(\exists_{h_1,h_2 \in H}(z = h_1xh_2y)) \implies (\exists_{h_3 \in H}(z = h_3xy))$

(3) $(\exists_{h_3 \in H}(z = h_3xy)) \implies \dots$

(3.1) $(NormalSubgroup[H,G,*]) \wedge (x \in G) \wedge (h_3 \in H)$ ▌ $x^{-1}h_3x \in H$

(3.2) $Group[H,*]$ ▌ $e \in H$

(3.3) $(e)x(x^{-1}h_3x)y = h_3xy = z$ ▌ $(e)x(x^{-1}h_3x)y = z$

(3.4) $(x^{-1}h_3x, e \in H) \wedge ((e)x(x^{-1}h_3x)y = h_3xy = z)$ ▌ $\exists_{h_1,h_2 \in H}(z = h_1xh_2y)$

(4) $(\exists_{h_3 \in H}(z = h_3xy)) \implies (\exists_{h_1,h_2 \in H}(z = h_1xh_2y))$

(5) $((\exists_{h_1,h_2 \in H}(z = h_1xh_2y)) \implies (\exists_{h_3 \in H}(z = h_3xy))) \wedge ((\exists_{h_3 \in H}(z = h_3xy)) \implies (\exists_{h_1,h_2 \in H}(z = h_1xh_2y)))$

(6) $(\exists_{h_1,h_2 \in H}(z = h_1xh_2y)) \iff (\exists_{h_3 \in H}(z = h_3xy))$

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

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

(1.1) $(NormalSubgroup[H,G,*]) \wedge (QuotientGroupLemma)$ ▌ $\forall_{x,y,z \in G}((\exists_{h_1,h_2 \in H}(z = h_1xh_2y)) \iff (\exists_{h_3 \in H}(z = h_3xy)))$

(1.2) $(z \in Hx \bar{*} Hy) \iff (\exists_{h_1,h_2 \in H}(z = h_1xh_2y)) \iff (\exists_{h_3 \in H}(z = h_3xy)) \iff (z \in Hxy)$ ▌ $Hx \bar{*} Hy = Hxy$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(5) $(g, h \in G) \implies \ldots$

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

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

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

(7) $\ldots (Func[\psi, G/ker_\phi, im_\phi]) \wedge (Inj[\psi, G/ker_\phi, im_\phi]) \wedge (Surj[\psi, G/ker_\phi, im_\phi])$ ▌ $Bij[\psi, G/ker_\phi, im_\phi]$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(8) $(N \subseteq HN) \wedge (Group[N, *])$ ▌ $Subgroup[N, HN, *]$

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

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

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

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

(12) $(SubgroupIntersection) \wedge (Subgroup[H, G, *]) \wedge (Subgroup[N, G, *])$ ▌ $Subgroup[H \cap N, G, *]$ ▌ $Group[H \cap N, *]$

(13) $(H \cap N \subseteq H) \wedge (Group[H \cap N, *])$ ▌ $Subgroup[H \cap N, H, *]$

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

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

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

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

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

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

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

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

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

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

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

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

(1) $SecondIsoLemma$ ▌ $(Group[(HN)/N, \bar{\ast}]) \wedge (Group[H/(H \cap N), \bar{\ast}])$

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

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

   (3.1) $\phi(h_1) = h_1 N = h_2 N = \phi(h_2)$ ▌ $\phi(h_1) = \phi(h_2)$

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

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

   (5.1) $\phi(h_1 * h_2) = (h_1 * h_2)N = (h_1 N) \bar{\ast} (h_1 N) = \phi(h_1) \bar{\ast} \phi(h_2)$ ▌ $\phi(h_1 * h_2) = \phi(h_1) \bar{\ast} \phi(h_2)$

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

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

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

(9) $im_\phi = \{\phi(h) \mid h \in H\} = \{hN \mid h \in H\} = (HN)/N$ ▌ $im_\phi = (HN)/N$

(10) $(FirstMapThm) \wedge (Homomorphism[\phi, H, *, (HN)/N, \bar{\ast}])$ ▌ $Isomorphic[H/ker_\phi, \bar{\ast}, im_\phi, \bar{\ast}]$

(11) $(ker_\phi = H \cap N) \wedge (im_\phi = (HN)/N) \wedge (Isomorphic[H/ker_\phi, \bar{\ast}, im_\phi, \bar{\ast}])$ ▌ $Isomorphic[H/(H \cap N), \bar{\ast}, (HN)/N, \bar{\ast}]$

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

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

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

(2) $((g_1 K, g_2 K \in (G/K)) \wedge (g_1 K = g_2 K)) \implies \ldots$

   (2.1) $g_1 K = g_2 K$ ▌ $(g_2)^{-1} g_1 K = K$ ▌ $(g_2)^{-1} g_1 \in K$

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

   (2.3) $(g_2)^{-1} g_1 \in H$ ▌ $g_1 H = g_2 H$ ▌ $\phi(g_1 K) = g_1 H = g_2 H = \phi(g_2 K)$ ▌ $\phi(g_1 K) = \phi(g_2 K)$

(3) $((g_1 K, g_2 K \in (G/K)) \wedge (g_1 K = g_2 K)) \implies (\phi(g_1 K) = \phi(g_2 K))$ ▌ $\forall_{g_1 K, g_2 K \in (G/K)}((g_1 K = g_2 K) \implies (\phi(g_1 K) = \phi(g_2 K))) \ldots$

(4) $\ldots Func[\phi, G/K, G/H]$

(5) $(g_1 K, g_2 K \in (G/K)) \implies \ldots$

   (5.1) $\phi(g_1 K \bar{\ast} g_2 K) = \phi((g_1 * g_2)K) = (g_1 * g_2)H = (g_1 H) \bar{\ast} (g_2 H) = \phi(g_1 K) \bar{\ast} \phi(g_2 K)$ ▌ $\phi(g_1 K \bar{\ast} g_2 K) = \phi(g_1 K) \bar{\ast} \phi(g_2 K)$

(6) $(g_1 K, g_2 K \in (G/K)) \implies (\phi(g_1 K \bar{\ast} g_2 K) = \phi(g_1 K) \bar{\ast} \phi(g_2 K))$ ▌ $\forall_{g_1 K, g_2 K \in (G/K)}(\phi(g_1 K \bar{\ast} g_2 K) = \phi(g_1 K) \bar{\ast} \phi(g_2 K))$

(7) $(Func[\phi, G/K, G/H]) \wedge (\forall_{g_1 K, g_2 K \in (G/K)}(\phi(g_1 K \bar{\ast} g_2 K) = \phi(g_1 K) \bar{\ast} \phi(g_2 K)))$ ▌ $Homomorphism[\phi, G/K, \bar{\ast}, G/H, \bar{\ast}]$

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

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

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

   (9.2) $g \in G$ ▌ $gK \in (G/K)$

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

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

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

(11) $(SurjEquiv) \wedge (Surj[\phi, G/K, G/H])$ ▌ $im_\phi = G/H$

(12) $(FirstMapThm) \wedge (Homomorphism[\phi, G/K, \bar{\ast}, G/H, \bar{\ast}])$ ▌ $Isomorphic[(G/K)/ker_\phi, \bar{\ast}, im_\phi, \bar{\ast}]$

(13) $(ker_\phi = H/K) \wedge (im_\phi = G/H) \wedge (Isomorphic[(G/K)/ker_\phi, \bar{\ast}, im_\phi, \bar{\ast}])$ ▌ $Isomorphic[(G/K)/(H/K), \bar{\ast}, G/H, \bar{\ast}]$