Contents

Chapter 1

Graph Theory

1.1 Graphs

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

$VertexSet[V((V,E)),(V,E)] := \left(SimpleGraph[(V,E)]\right) \wedge \left(V((V,E)) = V\right)$

$EdgeSet[E((V,E)),(V,E)] := \left(GrSimpleGraphaph[(V,E)]\right) \wedge \left(E((V,E)) = E\right)$

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

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

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

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

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

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

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

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

$kPartiteG[G,k] := \exists_S\left((|S| = k) \wedge \left(\forall_{S \in S}(IndependentSet[S,G])\right) \wedge \left(V(G) = \dot{\bigcup_{S \in S}}(S)\right)\right)$

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

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

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

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

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

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

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

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

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

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

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

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

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

$$IsomorphismEqRel := \forall_{G_1,G_2,G_3} \begin{pmatrix} (G_1 \cong G_1) & \wedge & \\ ((G_1 \cong G_2) \implies (G_2 \cong G_1)) & & \wedge \\ (((G_1 \cong G_2) \wedge (G_2 \cong G_3)) \implies (G_1 \cong G_3)) & & \end{pmatrix}$$

---

(1)   Bijection and composition properties

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

$PathN[P_n, n] := (PathG[P_n]) \wedge (|P_n| = n)$
$CycleN[C_n, n] := (CycleG[C_n]) \wedge (|C_n| = n)$
$CompleteN[K_n, n] := (CompleteG[K_n]) \wedge (|K_n| = n)$
$BicliqueRS[K_{r,s}, r, s] := (CompleteBipartiteG[K_{r,s}]) \wedge (PartiteSets[\{R, S\}, G]) \wedge (|R| = r) \wedge (S = s)$

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

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

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

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

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

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

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

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

$VCycle[W, G] := (Walk[W, G]) \wedge (w_{|W|} = w_1) \wedge \left(\forall_{i,j \in \mathbb{N}_2^{|W|-1}}\left((i \neq j) \implies (w_i \neq w_j)\right)\right)$
$xyWalk[(x, y), W, G] := (VWalk[W, G]) \wedge (W_1 = x) \wedge (W_{|W|} = y)$
$xyTrail[(x, y), W, G] := (VTrail[W, G]) \wedge (W_1 = x) \wedge (W_{|W|} = y)$
$xyPath[(x, y), W, G] := (VPath[W, G]) \wedge (W_1 = x) \wedge (W_{|W|} = y)$
$VLength[len(W), W, G] := (Walk[W, G]) \wedge \left(l(W) = |W| - 1\right)$
$VClosed[W, G] := (Walk[W, G]) \wedge (w_0 = w_{|W|})$
$VOdd[W, G] := (Walk[W, G]) \wedge \left(Odd(len(W))\right)$
$VEven[W, G] := (Walk[W, G]) \wedge \left(Even(len(W))\right)$
$PathInWalk[P, W, G] := (VPath[P, G]) \wedge (VWalk[W, G]) \wedge \exists_\phi \left((OrderedDeletion[\phi, W]) \wedge (P = \phi(W))\right)$
$CycleInWalk[C, W, G] := (VCycle[C, G]) \wedge (VWalk[W, G]) \wedge \exists_\phi \left((OrderedDeletion[\phi, W]) \wedge (C = \phi(W))\right)$

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

---

(1) $(l(W) = 0) \implies (P = W)$ ▌ $PathInWalk[P, W, G]$

---

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

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

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

(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. ▌ $PathInWalk[P', W, G]$

---

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

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

---

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

(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, $n - k \leq |mathcal H|$

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

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

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

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

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

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

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

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

---

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

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

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

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

  (4.1) $\exists_P\left((PathG[P]) \wedge (Subgraph[P,H-e])\right)$ ▌ $P+e$ must contain a cycle ▌ $\exists_C\left(((CycleG[C]) \wedge Subgraph[C,G]) \wedge \left(e\in E(C)\right)\right)$

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

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

  (6.1) $Component[H,G]$ ▌ $Connected[H]$

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

    (6.2.1) $\exists_P\left(xyPath[(u,v),P,H]\right)$

    (6.2.2) $(e\notin E(P)) \implies \left(\exists_P\left(xyPath[(u,v),P,H]\right)\right)$

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

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

      (6.2.3.2) $xyPath[(u,v),P',H-e]$ ▌ $\exists_P\left(xyPath[(u,v),P,H]\right)$

(6.2.4) $\left(e \in E(P)\right) \implies \left(\exists_P\big(xyPath[(u,v), P, H]\big)\right)$

(6.2.5) $\exists_P\big(xyPath[(u,v), P, H]\big)$

(6.3) $\left(u,v \in V(H)\right) \implies \left(\exists_P\big(xyPath[(u,v), P, H-e]\big)\right)$ ▮ $Connected[H-e]$

(7) $\left(\exists_C\Big(\big((CycleG[C]) \wedge Subgraph[C,G]\big) \wedge \big(e \in E(C)\big)\Big)\right) \implies (Connected[H-e])$

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

(1) $(len(W) = 1) \implies (W = C)$ ▮ $\exists_C((VCycle[C,G]) \wedge (VOdd[C,G]) \wedge (CycleInWalk[C,W,G]))$

(2) $\big((len(W) > 1)\big) \wedge \big(\forall_{W'}((len(W') < len(W)) \implies$

$\Big(((VClosed[W',G]) \wedge (VOdd[W',G])) \implies \big(\exists_{C'}((VCycle[C',G]) \wedge (VOdd[C',G]) \wedge (CycleInWalk[C',W',G]))\big)\Big)\big)\big))) \implies \dots$

   (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) $\big((len(W) > 1)\big) \wedge \big(\forall_{W'}((len(W') < len(W)) \implies$

$\Big(((VClosed[W',G]) \wedge (VOdd[W',G])) \implies \big(\exists_{C'}((VCycle[C',G]) \wedge (VOdd[C',G]) \wedge (CycleInWalk[C',W',G]))\big)\Big)\big)\big))) \implies$

$(\exists_C((VCycle[C,G]) \wedge (VOdd[C,G]) \wedge (CycleInWalk[C,W,G])$

(4) By induction: $\exists_C\big((VCycle[C,G]) \wedge (VOdd[C,G]) \wedge (CycleInWalk[C,W,G])\big)$

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

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

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

(2) $(Bipartite[G]) \implies \left(\neg\exists_C((CycleG[C]) \wedge (Subgraph[C,G]) \wedge (VOdd[C,G]))\right)$

(3) $\left(\neg\exists_C((CycleG[C]) \wedge (Subgraph[C,G]) \wedge (VOdd[C,G]))\right) \implies \dots$

   (3.1) Consider each nontrivial component H, and pick a $u \in V(H)$.

   (3.2) Let $X = \{v \in H \mid Even(d(v,u))\}$ and let $Y = \{v \in H \mid Odd(d(v,u))\}$.

   (3.3) Suppose X or Y are not independent sets. WLOG choose X.

     (3.3.1) X must contain an edge - call it $\{v,v'\}$

     (3.3.2) A closed odd walk could be: min u-v path (+ even) and v-v' (+ 1) and min v'-u path (+ even)

     (3.3.3) By $OddCycleInClosedOddWalk$, there exists an odd cycle in G. ▮ $\bot$

   (3.4) X and Y are independent sets; futhermore X, Y are bipartitions of G. ▮ $Bipartite[G]$

(4) $\left(\neg\exists_C((CycleG[C]) \wedge (Subgraph[C,G]) \wedge (VOdd[C,G]))\right) \implies (Bipartite[G])$

(5) $(Bipartite[G]) \iff \left(\neg\exists_C((CycleG[C]) \wedge (Subgraph[C,G]) \wedge (VOdd[C,G]))\right)$

TODO: verify "contains in" definition

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

---

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

---

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

---

(3) $\Big(\forall_{v\in V(G)}\big(Even(d(v))\big)\Big) \implies ...$

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

(3.2) $\big(e(G) \neq 0\big) \implies ...$

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

(3.2.2)   There exists a Path P of maximal length with endvertices (x_0, x_l).

(3.2.3) $\big(d(x_0) \geq 2\big)$ $\blacksquare$ 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 $G' = G - E(C)$. $\blacksquare$ $\Big(\forall_{v\in V(G')}\big(Even(d_{G'}(v))\big)\Big)$ $\blacksquare$ Repeat on G' until all disjoint cycles $\mathcal{C}$ are found.

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

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

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

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

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

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

(1) $\left(\neg \exists_W (Triangle[W, G]) \right) \implies \ldots$

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

(1.4) $\sum_{v \in V(G)} \left((d(v))^2 \right) \leq n(e(G))$ ▮ $n \sum_{v \in V(G)} \left((d(v))^2 \right) \leq n^2(e(G))$

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

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

(1.7) $\left(e(G) > \left\lfloor n^2/4 \right\rfloor \right) \wedge \left(e(G) \leq n^2/4 \right)$ ▮ $\bot$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$\boxed{[\text{Notation}] \quad (K(n_1, ..., n_r)) := Complete\,RpartiteG}$

$\boxed{[\text{Notation}] \quad (K_r(t)) := K(t, ..., t)}$

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

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

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

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

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

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

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

---

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

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

---

(1) $\quad$ SumDeg

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

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

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

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

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

---

(1) $\quad$ TODO $\phi = \dots$

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

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

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

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

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

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

$KroneckerProperties := \dots$

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

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

(1)   TODO

acyclic graph

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

forest -> decomponents into trees

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

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

(1)   TODO

Chapter 2

Abstract Algebra

2.1 Functions

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

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

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

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

(1)	TODO

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

(1)	TODO

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

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

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

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

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

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

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

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

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

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

(1)	TODO

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

(1)	TODO

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

(1)	TODO

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

(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

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

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

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

$RelPrime[a, b] := GCD[1, a, b]$

$CongRel[a, b, n] := Divides[n, a - b]$

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

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

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

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

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

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

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

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

(1)   TODO

2.3   Groups

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

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

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

---

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

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

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

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

(3.1)   TODO

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

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

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

---

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

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

(1) $(Cancel Laws) \wedge \left(\forall_{a \in G} \exists_{a^{-1} \in G} (a * a^{-1} = e = a^{-1} * a) \right)$ ▌ $a * a_1^{-1} = e = a * a_2^{-1}$ ▌ $a_1^{-1} = a_2^{-1}$

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

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

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

(3) $InvUniq$ ▌ $(a * b)^{-1} = b^{-1} * a^{-1}$

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

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

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

2.4   Subgroups

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

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

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

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

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

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

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

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

  (2.6) $Group[H, *]$

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

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

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

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

(1) TODO

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

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

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

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

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

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

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

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

(5)	$\left(a \in C(g) \right) \implies \ldots$

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

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

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

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

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

2.5   Special Groups

2.5.1   Cyclic Group

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

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

(1)	$\exists_{g \in G} (Generator[g, G, *])$

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

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

(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)	$(g^r \in H) \wedge (0 \leq r < m) \wedge \left(\forall_{k \in \mathbb{Z}^+} \big((k < m) \implies (g^k \notin H) \big) \right)$ ▮ $r = 0$
(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)	$\exists_{k \in \mathbb{Z}} \big(b = (g^m)^k \big)$
(5.2)	$(Group[H, G, *]) \wedge (g^m \in H)$ ▮ $(g^m * g^m \in H) \wedge \left((g^m)^{-1} \in H \right)$
(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)	$(H \subseteq <g^m>) \wedge (<g^m> \subseteq H)$ ▮ $H = <g^m>$ ▮ $Generator[g^m, H, *]$ ▮ $\exists_{h \in G}(Generator[h, G, *])$ ▮ $CyclicGroup[H, *]$

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

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

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

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

2.5.2 Symmetric and Alternating Groups

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

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

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

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

2.5.3 Dihedral Group

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

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

2.6   Lagrange's Theorem

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

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

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

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

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

  (1.3) $\big((a \sim b) \land (b \sim c)\big) \implies (a * b^{-1}, b * c^{-1} \in H) \implies \Big(a * c^{-1} = (a * b^{-1}) * (b * c^{-1}) \in H\Big)$ ▐ $a \sim c$

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

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

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

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

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

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

(1) $(CosetInduceEqRel) \land (EqRelInducesPartition) \land (CosetCardinality)$ ▐ $\big(o(G) = o(H)|G : H|\big) \land \big(Divides[o(H), o(G)]\big)$

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

(1) $CyclicSubgroup[<g>, g, G, *]$ ▐ $Order[<g>] = m$

(2) $(LagrangeTheorem) \land (CyclicSubgroup)$ ▐ $Divides[Order[<g>], Order[G]]$ ▐ $Divides[m, n]$

(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

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

(1) $(LagrangeTheorem) \land (SubgroupIntersection) \land \Big(RelPrime\big(o(H), o(K)\big)\Big)$ ▐ $H \cap K = \{e\}$

2.7   Homomorphisms

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

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

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

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

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

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

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

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

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

(3) $\quad \Big(\forall_{m \in \mathbb{N}^+}\big((m \le n) \implies \big(\phi(g^m) = \phi(g)^m\big)\big)\Big) \implies \dots$

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

(4) $\quad \Big(\forall_{m \in \mathbb{N}^+}\big((m \le n) \implies \big(\phi(g^m) = \phi(g)^m\big)\big)\Big) \implies \big(\phi(g^{n+1}) = \phi(g)^{n+1}\big)$

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

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

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

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

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

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

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

(1) $\quad Inj[\phi, G, H]$ ▌ $\forall_{g_1, g_2 \in G}\Big(\big(\phi(g_1) = \phi(g_2)\big) \implies (g_1 = g_2)\Big)$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3.2) $\phi^{-1}(x \diamond y) = \phi^{-1}\Big(\phi\Big(\phi^{-1}(x) * \phi^{-1}(y)\Big)\Big) = (\phi^{-1} \circ \phi)\Big(\phi^{-1}(x) * \phi^{-1}(y)\Big) = \phi^{-1}(x) * \phi^{-1}(y)$ ▌ $\phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y)$

(4) $(x, y \in H) \implies \Big(\phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y)\Big)$ ▌ $\forall_{x,y \in H}\Big(\phi^{-1}(x \diamond y) = \phi^{-1}(x) * \phi^{-1}(y)\Big)$

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

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

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

(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) $(ExpModOrder) \wedge (Order[n, G, *]) \wedge (Order[n, H, \diamond])$ ▌ $(g^{n_1} = g^{n_2}) \iff \left(n_1 \equiv n_2 (mod\ n)\right) \iff (h^{n_1} = h^{n_2}) \iff \ldots$

  (3.2) $\ldots \left(\phi(g^{n_1}) = \phi(g^{n_2})\right)$ ▌ $(g^{n_1} = g^{n_2}) \iff \left(\phi(g^{n_1}) = \phi(g^{n_2})\right)$

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

(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) $(g^n, g^m \in G) \implies \left(\phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m)\right)$ ▌ $\forall_{g^n, g^m \in G}\left(\phi(g^n * g^m) = \phi(g^n) \diamond \phi(g^m)\right)$

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

(9) $\exists_\phi(Isomorphism[\phi, G, *, H, \diamond])$ ▌ $Isomorphic[G, *, H, \diamond]$

2.8 Kernel and Image Homomorphisms

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

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

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

(1) $IdMapsId$ ▌ $\phi(e_G) = e_H$ ▌ $e_G \in ker_\phi$ ▌ $ker_\phi \neq \emptyset$

(2) $ker_\phi \subseteq G$ ▌ $\emptyset \neq ker_\phi \subseteq G$

(3) $(a, b \in ker_\phi) \implies \ldots$

  (3.1) $\left(\phi(a) = e_H\right) \wedge \left(\phi(b) = e_H\right)$ ▌ $\phi(a * b) = \phi(a) \diamond \phi(b) = e_H \diamond e_H = e_H$ ▌ $a * b \in ker_\phi$

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

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

(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) $(a, b \in im_\phi) \implies \ldots$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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) $(ker_\phi=\{e_G\})\implies\ldots$

(3.1) $\Big((g_1,g_2\in G)\wedge\big(\phi(g_1)=\phi(g_2)\big)\Big)\implies\ldots$

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

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

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

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

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

(1) $\Big(x\in(ker_\phi)g\Big)\implies\ldots$

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

(3) $\Big((x\in G)\wedge\big(\phi(x)=\phi(g)\big)\Big)\implies\ldots$

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

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

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

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

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

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

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

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

(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

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

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

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

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

  (1.4) $\dots \Big(c = x_c^{-1} * x_b^{-1} * a * x_b * x_c = (x_b * x_c)^{-1} * a * (x_b * x_c)\Big)$ ▮ $a \sim^* c$

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

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

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

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

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

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

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

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

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

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

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

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

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

  (3.3) $(x \in G) \implies \left(\Big(\exists_{c \in G}(x = c^{-1}gc)\Big) \iff (x \in \{g\})\right)$ ▮ $\forall_{x \in G}\Big((x \in \{g\}) \iff \big(\exists_{c \in G}(x = c^{-1}gc)\big)\Big)$

  (3.4) $(ConjugacyClassEquiv) \wedge \left(\forall_{x \in G}\Big((x \in \{g\}) \iff \big(\exists_{c \in G}(x = c^{-1}gc)\big)\Big)\right)$ ▮ $C_g = \{g\}$

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

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

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

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

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

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

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

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

(3) $\left[(n > 1) \wedge \left(\forall_{m \in \mathbb{N}^+}\left((m \le n) \implies \left((x^{-1}gx)^m = x^{-1}g^m x \right) \right) \right) \right] \implies \ldots$

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

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

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

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

(1) $\exists_{c \in G}(g_2 = c^{-1}g_1 c)$

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

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

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

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

(6) $\left(Divides[o(g_2), o(g_1)] \right) \wedge \left(Divides[o(g_1), o(g_2)] \right) \wedge (g_1, g_2 \in \mathbb{N}^+)$ ▌ $o(g_1) = o(g_2)$

(7) ==

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

(9) $(m \in \mathbb{Z}^+) \wedge \left(m < o(g_2) \right) \implies \ldots$

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

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

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

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

(1) $\left(c^{-1}ac \in c^{-1}C(g)c \right) \implies \ldots$

(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) $\left(c^{-1}ac \in c^{-1}C(g)c \right) \implies \left(c^{-1}ac \in C(h) \right)$ ▌ $c^{-1}C(g)c \subseteq C(h)$

(3) $\left(a \in C(h) \right) \implies \ldots$

(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) $\left(a \in C(h) \right) \implies \left(a \in c^{-1}C(g)c \right)$ ▌ $C(h) \subseteq c^{-1}C(g)c$

(5) $\left(c^{-1}C(g)c \subseteq C(h) \right) \wedge \left(C(h) \subseteq c^{-1}C(g)c \right)$ ▌ $C(h) = c^{-1}C(g)c$

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

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

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

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

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

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

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

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

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

2.10 Normal Subgroups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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) $(b \in H) \implies \Big(b \in C_b \subseteq \bigcup_{z \in H}(C_z)\Big)$ ▮ $(b \in H) \implies \Big(b \in \bigcup_{z \in H}(C_z)\Big)$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.11   Quotient Groups

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

$CosetMul[\bar{\mp}, H, G, *] := (Subgroup[H, G, *]) \wedge \left(\forall_{Hx, Hy \in G/H}(Hx \bar{\mp} Hy = \{h_1xh_2y \mid h_1, h_2 \in H\}) \right)$

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

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

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

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

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

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

 (1.4) $(h_1xh_2x^{-1})(xy) = h_1xh_2y = z \; \blacksquare \; (h_1xh_2x^{-1})(xy) = z$

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

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

(3) $\left(\exists_{h_3 \in H}(z = h_3xy) \right) \implies \ldots$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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) $\psi(ker_\phi g \; \bar{\ast} \; ker_\phi h) = \psi(ker_\phi gh) = \phi(g \ast h) = \phi(g) \diamond \phi(h) = \psi(ker_\phi g) \diamond \psi(ker_\phi h)$ ∎ $\psi(ker_\phi g \; \bar{\ast} \; ker_\phi h) = \psi(ker_\phi g) \diamond \psi(ker_\phi h)$

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

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

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

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

(1) $(Group[H, \ast]) \wedge (Group[N, \ast])$ ∎ $(e \in H) \wedge (e \in N)$

(2) $e = e \ast e \in HN$ ∎ $\emptyset \neq HN \subseteq G$

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

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

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

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

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

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

(8) $(N \subseteq HN) \wedge (Group[N, \ast])$ ∎ $Subgroup[N, HN, \ast]$

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

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

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

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

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

(13) $(H \cap N \subseteq H) \wedge (Group[H \cap N, \ast])$ ∎ $Subgroup[H \cap N, H, \ast]$

(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) $(Group[H, \ast]) \wedge (h \in H)$ ∎ $h^{-1} \in H$

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

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

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

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

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

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

(18) $QuotientGroupThm$ ▐ $\big(Group[(HN)/N, \bar{\ast}]\big) \wedge \big(Group[H/(H \cap N), \bar{\ast}]\big)$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(2) $\Big(\big((g_1 K, g_2 K \in (G/K)\big) \wedge (g_1 K = g_2 K)\Big) \implies \dots$

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

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

   (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) $\Big(\big((g_1 K, g_2 K \in (G/K)\big) \wedge (g_1 K = g_2 K)\Big) \implies \big(\phi(g_1 K) = \phi(g_2 K)\big)$ ▐ $\forall_{g_1 K, g_2 K \in (G/K)}\Big((g_1 K = g_2 K) \implies \big(\phi(g_1 K) = \phi(g_2 K)\big)\Big)$ $\dots$

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

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

   (5.1) $\phi(g_1 K \bar{\ast} g_2 K) = \phi\big((g_1 \ast g_2)K\big) = (g_1 \ast g_2)H = (g_1 H) \bar{\ast} (g_2 H) = \phi(g_1 K) \bar{\ast} \phi(g_2 K)$ ▐ $\phi(g_1 K \bar{\ast} g_2 K) = \phi(g_1 K) \bar{\ast} \phi(g_2 K)$

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

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

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

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

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

(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) $(ker_\phi = H/K) \wedge (im_\phi = G/H) \wedge \left(Isomorphic[(G/K)/ker_\phi, \bar{*}, im_\phi, \bar{*}] \right)$ ∎ $Isomorphic[(G/K)/(H/K), \bar{*}, G/H, \bar{*}]$