Contents

Chapter 1

Graph Theory

1.1 Graphs

1.1.1 **Graph operations**

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

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

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

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

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

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

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

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

1.1.2 Graphs

$$SimpleGraph[(V, E)] := (Set[V]) \wedge (E \subseteq \{\{a, b\} \in V^{\{2\}} \mid a \neq b\})$$
$$VertexSet[V\big((V, E)\big), (V, E)] := \big(SimpleGraph[(V, E)]\big) \wedge \Big(V\big((V, E)\big) = V\Big)$$
$$EdgeSet[E\big((V, E)\big), (V, E)] := \big(SimpleGraph[(V, E)]\big) \wedge \Big(E\big((V, E)\big) = E\Big)$$
$$AdjacentV[\{x, y\}, G] := \{x, y\} \in E(G)$$
$$Incident[e, x, y, G] := e = \{x, y\} \in E(G)$$
$$Degree[d(x), x, G] := d(x) = |\{y \in V(G) \mid AdjacentV[\{x, y\}, G]\}|$$
$$Order[n(G), G] := n(G) = |V(G)|$$
$$Size[e(G), G] := e(G) = |E(G)|$$

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

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

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

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

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

1.1.3 Paths, Cycles, Trails

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

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

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

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

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

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

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

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

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

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

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

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

(1) Bijection and composition properties

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

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

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

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

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

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

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

TODO: ADD SPECIAL GRAPHS

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

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

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

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

$Walk[W,G] := \left(\forall_{i\in\mathbb{N}_1^{|W|-1}}\left(\{w_i, w_{i+1}\} \in E(G)\right)\right)$
$EdgesWalk[E(W),W,G] := (Walk[W,G]) \wedge \left(E(W) = \{\{w_i, w_{i+1}\} \mid i \in \mathbb{N}_1^{|W|-1}\}\right)$
$Trail[W,G] := (Walk[W,G]) \wedge \left(\forall_{i,j\in\mathbb{N}_1^{|W|-1}}\left((i \neq j) \implies (\{w_i, w_{i+1}\} \neq \{w_j, w_{j+1}\})\right)\right)$
$uvWalk[(u,v),W,G] := (Walk[W,G]) \wedge (W_1 = u) \wedge (W_{|W|} = v)$
$uvTrail[(u,v),W,G] := (Trail[W,G]) \wedge (W_1 = u) \wedge (W_{|W|} = v)$
$uvPath[(u,v),P] := (PathG[P]) \wedge \left(u,v \in V(P)\right) \wedge \left(d(u) = 1 = d(v)\right)$
$LengthWalk[e(W),W,G] := (Walk[W,G]) \wedge \left(e(W) = |E(W)|\right)$
$ClosedWalk[W,G] := (Walk[W,G]) \wedge (w_1 = w_{|W|})$
$OddWalk[W,G] := (Walk[W,G]) \wedge \left(Odd\left(e(W)\right)\right)$
$EvenWalk[W,G] := (Walk[W,G]) \wedge \left(Even\left(e(W)\right)\right)$
$WalkContainsPath[P,W,G] := (Path[P]) \wedge (Walk[W,G]) \wedge \left(OrderedSublist[V(P),W]\right) \wedge \left(OrderedSublist[E(P),E(W)]\right)$
$WalkContainsCycle[C,W,G] := (Cycle[C]) \wedge (Walk[W,G]) \wedge \left(OrderedSublist[V(C),W]\right) \wedge \left(OrderedSublist[E(C),E(W)]\right)$

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

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

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

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

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

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

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

$ConnectedV[(x,y),G] := \exists_P\left((Subgraph[P,G]) \wedge \left(uvPath[(x,y),P]\right)\right)$
$Connected[G] := \forall_{x,y\in V(G)}\left(ConnectedV[(x,y),G]\right)$
$Connection[C_G,G] := C_G = \{\langle x,y\rangle \mid ConnectedV[(x,y),G]\}$

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

(1) By $(uvWalkContainsuvPath) \wedge \left(uvPath[(x,y),W]\right) \iff \left(uvPath[(y,x),W]\right)$

$ConnectedSubgraph[H,G] := (Subgraph[H,G]) \wedge (Connected[H])$
$Component[H,G] := ConnectedSubgraph[H,G] \wedge \left(\neg\exists_{K\neq H}\left((Subgraph[H,K]) \wedge (ConnectedSubgraph[K,G])\right)\right)$
$Trivial[G] := E(G) = \emptyset$
$Isolated[v,G] := d(v) = 0$

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

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

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

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

$$RemoveE[G-E,E,G] := \big(V(G-E)=V(G)\big) \wedge \big(E(G-E)=E(G)\setminus E\big)$$
$$AddE[G+e,e,G] := \Big(e \in V(G)^{\{2\}}\Big) \wedge \big(V(G+e)=V(G)\big) \wedge \big(E(G+e)=E(G)\cup\{e\}\big)$$
$$InducedSubgraph[G[T],T,G] := G[T]=G-\bar{T}$$
$$IndependentSet[S,G] := E(G[S])=\emptyset$$

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

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

---

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

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

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

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

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

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

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

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

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

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

(6.2.2) $\big(e\notin E(P)\big) \implies \ldots$

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

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

(6.2.4) $\big(e\in E(P)\big) \implies \ldots$

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

(6.2.4.2) $(Subgraph[P',H-e]) \wedge \big(uvPath[(u,v),P']\big) \blacksquare\ \exists_P\Big((Subgraph[P,H-e]) \wedge \big(uvPath[(u,v),P]\big)\Big)$

(6.2.5) $\big(e\in E(P)\big) \implies \Big(\exists_P\Big((Subgraph[P,H-e]) \wedge \big(uvPath[(u,v),P]\big)\Big)\Big)$

(6.2.6) $\exists_P\Big((Subgraph[P,H-e]) \wedge \big(uvPath[(u,v),P]\big)\Big)$

(6.3) $\big(u,v\in V(H)\big) \implies \Big(\exists_P\Big((Subgraph[P,H-e]) \wedge \big(uvPath[(u,v),P]\big)\Big)\Big) \blacksquare\ Connected[H-e]$

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

(8) $(Connected[H-e]) \iff \Big(\exists_C\Big((CycleG[C]) \wedge (Subgraph[C,G]) \wedge \big(e\in E(C)\big)\Big)\Big)$

$$COWalkContainsOCycle := \big((ClosedWalk[W,G]) \wedge (OddWalk[W,G])\big) \implies \bigg(\exists_C\Big((WalkContainsCycle[C,W,G]) \wedge \Big(Odd\big(e(C)\big)\Big)\Big)\bigg)$$

---

(1) $\big(e(W)=1\big) \implies \big(C=(\{w_1\},\emptyset)\big) \blacksquare\ \exists_C\Big((WalkContainsCycle[C,W,G]) \wedge \Big(Odd\big(e(C)\big)\Big)\Big)$

(2) $\big((e(W)>1\big) \wedge \big(\forall_{W'}((e(W')<e(W)\big) \implies$
$\Bigg(\big((ClosedWalk[W',G]) \wedge (OddWalk[W',G])\big) \implies \bigg(\exists_{C'}\Big((WalkContainsCycle[C',W',G]) \wedge \Big(Odd\big(e(C')\big)\Big)\Big)\bigg)\Bigg))) \implies \ldots$

(2.1) If W has no repeated vertex other than the first and last, then $C = \left(W, E(W)\right)$ $\blacksquare$ $\exists_C\left((WalkContainsCycle[C, W, G]) \land \left(Odd\left(e(C)\right)\right)\right)$

(2.2) If W has a repeated vertex v, then ...

(2.2.1) Break W into two v Walks W_1, W_2. Since W is odd, W_1, W_2 are odd and even walks (not in order).

(2.2.2) WLOG let W_1 be the odd subwalk, then by IH $\exists_{C'}\left((WalkContainsCycle[C', W_1, G]) \land \left(Odd\left(e(C')\right)\right)\right)$

(2.2.3) $\exists_C\left((WalkContainsCycle[C, W, G]) \land \left(Odd\left(e(C)\right)\right)\right)$

(2.3) If W has a repeated vertex v, then $\exists_C\left((WalkContainsCycle[C, W, G]) \land \left(Odd\left(e(C)\right)\right)\right)$

(2.4) $\exists_C\left((WalkContainsCycle[C, W, G]) \land \left(Odd\left(e(C)\right)\right)\right)$

(3) $\left((e(W) > 1\right) \land \left(\forall_{W'}((e(W') < e(W)\right) \implies$ $\left(((ClosedWalk[W', G]) \land (OddWalk[W', G])) \implies \left(\exists_{C'}\left((WalkContainsCycle[C', W', G]) \land \left(Odd\left(e(C')\right)\right)\right)\right)\right))) \implies$ $\left(\exists_C\left((WalkContainsCycle[C, W, G]) \land \left(Odd\left(e(C)\right)\right)\right)\right)$

(4) By induction: $\exists_C\left((WalkContainsCycle[C, W, G]) \land \left(Odd\left(e(C)\right)\right)\right)$

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

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

(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) $\neg\exists_C\left((CycleG[C]) \land (Subgraph[C, G]) \land \left(Odd\left(e(C)\right)\right)\right)$

(2) $(Bipartite[G]) \implies \left(\neg\exists_C\left((CycleG[C]) \land (Subgraph[C, G]) \land \left(Odd\left(e(C)\right)\right)\right)\right)$

(3) $\left(\neg\exists_C\left((CycleG[C]) \land (Subgraph[C, G]) \land \left(Odd\left(e(C)\right)\right)\right)\right) \implies \ldots$

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

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

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

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

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

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

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

(4) $\left(\neg\exists_C\left((CycleG[C]) \land (Subgraph[C, G]) \land \left(Odd\left(e(C)\right)\right)\right)\right) \implies (Bipartite[G])$

(5) $(Bipartite[G]) \iff \left(\neg\exists_C\left((CycleG[C]) \land (Subgraph[C, G]) \land \left(Odd\left(e(C)\right)\right)\right)\right)$

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

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

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

(1.1) $\left(\exists_{\langle B \rangle_1^k} \left(\left(\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B]) \right) \wedge (UnionG[K_n, \langle B \rangle_1^k]) \right) \right) \iff (Bipartite[K_n])$

(1.2) $(n \leq 2^k) \implies \ldots$

(1.2.1) $n \leq 2^1 = 2$ ▮ $\big((n = 1) \vee (n = 2)\big)$

(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) $(Bipartite[K_n]) \implies \ldots$

(1.4.1) $(n > 2) \implies \ldots$

(1.4.1.1) K_n has an odd cycle

(1.4.1.2) $BipartiteEquiv$ and K_n has an odd cycle ▮ $\neg Bipartite[K_n]$ ▮ $\perp$

(1.4.2) $(n > 2) \implies (\perp)$ ▮ $n \leq 2$

(1.5) $(Bipartite[K_n]) \implies (n \leq 2)$

(1.6) $(Bipartite[K_n]) \iff (n \leq 2)$ ▮ $\left(\exists_{\langle B \rangle_1^k} \left(\left(\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B]) \right) \wedge (UnionG[K_n, \langle B \rangle_1^k]) \right) \right) \iff (n \leq 2)$

(2) $(k = 1) \implies \left(\left(\exists_{\langle B \rangle_1^k} \left(\left(\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B]) \right) \wedge (UnionG[K_n, \langle B \rangle_1^k]) \right) \right) \iff (n \leq 2) \right)$

(3) $\left((k > 1) \wedge \left(\forall_{k'} \left((k' < k) \implies \left(\left(\exists_{\langle B \rangle_1^{k'}} \left(\left(\forall_{B \in \langle B \rangle_1^{k'}} (BipartiteG[B]) \right) \wedge (UnionG[K_n, \langle B \rangle_1^{k'}]) \right) \right) \iff (n \leq 2^{k'}) \right) \right) \right) \right) \implies \ldots$

(3.1) $\left(\exists_{\langle B \rangle_1^k} \left(\left(\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B]) \right) \wedge (UnionG[K_n, \langle B \rangle_1^k]) \right) \right) \implies \ldots$

(3.1.1) $K_n = \cup(\langle B \rangle_1^k) = \bigcup_{i=1}^{k} (B_i) = \bigcup_{i=1}^{k-1} (B_i) \cup B_k$ ▮ $K_n = \bigcup_{i=1}^{k-1} (B_i) \cup B_k$

(3.1.2) $Bipartite[B_k]$ ▮ $\exists_{X_0, Y_0} (PartiteSets[\{X_0, Y_0\}, B_k])$ ▮ $\exists_{X,Y} \Big(PartiteSets[\{X, Y\}, \big(V(G), E(B_k)\big)] \Big)$

(3.1.3) $K_n = \left(\bigcup_{i=1}^{k-1} (B_i) \cup B_k \right) \wedge (PartiteSets[\{X, Y\}, B_k])$ ▮ $\bigcup_{i=1}^{k-1} (B_i) = K_n[X] \cup K_n[Y]$

(3.1.4) $\bigcup_{i=1}^{k-1} (B_i) = K_n[X] \cup K_n[Y]$ and IH ▮ $\Big(|X| = n(K_n[X]) \leq 2^{k-1} \Big) \wedge \Big(|Y| = n(K_n[Y]) \leq 2^{k-1} \Big)$

(3.1.5) $n = |G| = |X| + |Y| \leq 2^{k-1} + 2^{k-1} = 2^k$ ▮ $n \leq 2^k$

(3.2) $\left(\exists_{\langle B \rangle_1^k} \left(\left(\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B]) \right) \wedge (UnionG[K_n, \langle B \rangle_1^k]) \right) \right) \implies (n \leq 2^k)$

(3.3) $(n \leq 2^k) \implies \ldots$

(3.3.1) $\exists_{X,Y} \Big(\big(X \dot{\cup} Y = V(K_n) \big) \wedge (|X| \leq 2^{k-1}) \wedge (|Y| \leq 2^{k-1}) \Big)$

(3.3.2) IH ▮ $\left(\exists_{\langle X \rangle_1^{k-1}} \left(\left(\forall_{X \in \langle X \rangle_1^{k-1}} (BipartiteG[X]) \right) \wedge (UnionG[K_n[X], \langle X \rangle_1^{k-1}]) \right) \right) \wedge$
$\left(\exists_{\langle Y \rangle_1^{k-1}} \left(\left(\forall_{Y \in \langle Y \rangle_1^{k-1}} (BipartiteG[Y]) \right) \wedge (UnionG[K_n[Y], \langle Y \rangle_1^{k-1}]) \right) \right)$

(3.3.3) $(\langle Z \rangle_1^{k-1} = \langle X_i \cup Y_i \rangle_{i=1}^{k-1}) \wedge (CompleteBipartiteG[Z_k, X, Y])$ ▮ $\left(\forall_{Z \in \langle Z \rangle_1^k} (BipartiteG[Z]) \right) \wedge (UnionG[K_n, \langle Z \rangle_1^k])$

(3.4) $(n \leq 2^k) \implies \left(\exists_{\langle B \rangle_1^k} \left(\left(\forall_{B \in \langle B \rangle_1^k} (BipartiteG[B]) \right) \wedge (UnionG[K_n, \langle B \rangle_1^k]) \right) \right)$

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

(4) $\left((k>1)\wedge\left(\forall_{k'}\left((k'<k)\implies\left(\left(\exists_{\langle B\rangle_1^k}\left((|\langle B\rangle_1^k|=k')\wedge\left(\forall_{B\in\langle B\rangle_1^k}(BipartiteG[B])\right)\wedge(UnionG[K_n,\langle B\rangle_1^k])\right)\right)\iff(n\leq 2^{k'})\right)\right)\right)\right)\implies$ $\left(\exists_{\langle B\rangle_1^k}\left(\left(\forall_{B\in\langle B\rangle_1^k}(BipartiteG[B])\right)\wedge(UnionG[K_n,\langle B\rangle_1^k])\right)\right)\iff(n\leq 2)$

(5) By induction: $\left(\exists_{\langle B\rangle_1^k}\left(\left(\forall_{B\in\langle B\rangle_1^k}(BipartiteG[B])\right)\wedge(UnionG[K_n,\langle B\rangle_1^k])\right)\right)\iff(n\leq 2)$

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

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

$MaximalPath[P,G] := (Subgraph[P,G])\wedge(PathG[P])\wedge\left(\neg\exists_{P'\neq P}((Subgraph[P,P'])\wedge(Subgraph[P',G])\wedge(PathG[P'])\right)$
$MaximalTrail[W,G] := (Trail[W,G])\wedge\left(\neg\exists_{W'\neq W}\left((W\subseteq W')\wedge(Trail[W',G])\right)\right)$
$VertexDegreeCycle := \left(\forall_{v\in V(G)}\left(2\leq d(v)\right)\right)\implies\left(\exists_C\left((Subgraph[C,G])\wedge(CycleG[C])\right)\right)$

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

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

(1) $(Eulerian[G])\implies\ldots$
(1.1) $Eulerian[G]$ $\blacksquare$ $\exists_W(EulerianCircuit[W,G])$
(1.2) The first and last vertices have even degree, and the intermediate vertices have even degree. $\blacksquare$ $EvenGraph[G]$
(1.3) $E(G)$ must be covered by the W, thus they must lie on the same non-trivial component. $\blacksquare$ $(\nexists\vee\exists!)_{H\in\mathcal{H}}(\neg Trivial[H])$
(1.4) $\left((\nexists\vee\exists!)_{H\in\mathcal{H}}(\neg Trivial[H])\right)\wedge(EvenGraph[G])$
(2) $(Eulerian[G])\implies\left(\left((\nexists\vee\exists!)_{H\in\mathcal{H}}(\neg Trivial[H])\right)\wedge(EvenGraph[G])\right)$
(3) $\left(\left((\nexists\vee\exists!)_{H\in\mathcal{H}}(\neg Trivial[H])\right)\wedge(EvenGraph[G])\right)\implies\ldots$
(3.1) $\left(E(G)=0\right)\implies\ldots$
(3.1.1) Let the Eulerian circuit be consist of just one vertex. $\blacksquare$ $Eulerian[G]$
(3.2) $\left(E(G)=0\right)\implies(Eulerian[G])$
(3.3) $\left(\left(E(G)>0\right)\wedge\left(\forall_{G'}\left(\left(E(G')<E(G)\right)\implies(Eulerian[G'])\right)\right)\right)\implies\ldots$
(3.3.1) $\exists!_H(H\in\mathcal{H}\mid\neg Trivial[H])$
(3.3.2) $EvenGraph[G]$ $\blacksquare$ $EvenGraph[H]$ $\blacksquare$ $\forall_{v\in V(H)}\left(2\leq d(v)\right)$
(3.3.3) $VertexDegreeCycle$ $\blacksquare$ $\exists_C\left((Subgraph[C,H])\wedge(CycleG[C])\right)$
(3.3.4) $G' := G - E(C)$
(3.3.5) Since the vertices in a cycle have degree 2, $EvenGraph[G']$. Each H' component of G' is also an $EvenGraph[H']$.

(3.3.6) By IH and $\forall_{H' \in \mathcal{H}'}\big(E(H') < E(G)\big) \;\blacksquare\; \forall_{H' \in \mathcal{H}'}(Eulerian[H'])$

(3.3.7) The Eulerian circuit of G can be constructed by:

(3.3.7.1) Start at some vertex in C

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

(3.3.7.3) Trail around H' using it's own Eulerian trail, and return to the vertex in C'.

(3.3.7.4) Continue the last two steps until the trail of C is complete.

(3.3.8) $Eulerian[G]$

(3.4) $\Big(\big(E(G) > 0\big) \wedge \Big(\forall_{G'}\Big(\big(E(G') < E(G)\big) \implies (Eulerian[G'])\Big)\Big)\Big) \implies \big((Eulerian[G])\big)$

(4) $\Big(\big((\nexists \vee \exists!)_{H \in \mathcal{H}}(\neg Trivial[H])\big) \wedge (EvenGraph[G])\Big) \implies (Eulerian[G])$

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

(1) $\big(E(G) = 0\big) \implies \ldots$

(1.1) $\mathcal{D} = \{G\} \;\blacksquare\; \exists_{\mathcal{D}}\Big((Decomposition[\mathcal{D}, G]) \wedge \big(\forall_{D \in \mathcal{D}}(Cycle[D])\big)\Big)$

(2) $\Bigg(\big(E(G) > 0\big) \wedge \Bigg(\forall_{G'}\Bigg(\big(E(G') < E(G)\big) \implies \Bigg((EvenGraph[G']) \implies \Big(\exists_{\mathcal{D}'}\Big((Decomposition[\mathcal{D}', G']) \wedge \big(\forall_{D' \in \mathcal{D}'}(Cycle[D'])\big)\Big)\Big)\Bigg)\Bigg)\Bigg)\Bigg)$
$\implies \ldots$

(2.1) $\big(E(G) > 0\big) \wedge (EvenGraph[G]) \;\blacksquare\; \forall_{v \in V(G)}\big(2 \le d(v)\big)$

(2.2) $VertexDegreeCycle \;\blacksquare\; \exists_C\big((Subgraph[C, G]) \wedge (CycleG[C])\big)$

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

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

(2.5) $E(D') < E(G)$ and IH, there exists a cycle decomposition of D'.

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

(2.7) $\exists_{\mathcal{D}}\Big((Decomposition[\mathcal{D}, G]) \wedge \big(\forall_{D \in \mathcal{D}}(Cycle[D])\big)\Big)$

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

(4) By induction, $\exists_{\mathcal{D}}\Big((Decomposition[\mathcal{D}, G]) \wedge \big(\forall_{D \in \mathcal{D}}(Cycle[D])\big)\Big)$

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

(1) $\exists_P(MaximalPath[P, G]) \;\blacksquare\; \exists_{u,v}\big(uvPath[(u, v), P]\big)$

(2) Since P is maximal, adjacent vertices of u must be contained in P.

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

(4) Thus P has at least k vertices. $\blacksquare\; k \le E(P)$.

(5) $\exists_P\Big((Subgraph[P, G]) \wedge (PathG[P]) \wedge \big(k \le e(P)\big)\Big)$

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

(1) $VertexDegreePathk \;\blacksquare\; \exists_P\Big((Subgraph[P, G]) \wedge (PathG[P]) \wedge \big(k \le e(P)\big)\Big)$

(2) The edge formed by u and it's farthest neighbor along P will form a cycle C with $k + 1 \le e(C)$

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

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

(1) $\exists_P(MaximalPath[P,G])$ ▮ $\exists_{u,v}\left(uvPath[(u,v),P]\right)$

(2) $Connected[P-u]$ ▮ $\neg CutVertex[u,G]$

(3) $(v \neq u) \implies (\neg CutVertex[v,G])$

(4) $(v = u) \implies \ldots$ ▮ Take another maximal path within $P-u$. ▮ Take another endpoint u'. ▮ $\neg CutVertex[u',G]$

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

(1) Every step in W adds 1 degree to each endpoint.

(2) Thus when arriving at a vertex u that is not the initial vertex, u will have an odd count of edges incident to it.

(3) Since u has an even degree, then there remains an edge where W can continue.

(4) Therefore, the W can only end (become maximal) when it reaches it's initial vertex. ▮ $ClosedWalk[W,G]$

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

(1) $(k = 0) \implies \ldots$

(1.1) $k = 0$ ▮ $EvenGraph[G]$

(1.2) $Connected[G]$ ▮ $\exists!_{H \in \mathcal{H}}(\neg Trivial[H])$

(1.3) $EulerianEquiv$ ▮ $Eulerian[G]$ ▮ $\exists_W(EulerianCircuit[W,G])$

(1.4) $D := \left(V(G), E(W)\right)$ ▮ $(Trail[D,G]) \wedge (Decomposition[\{D\},G]) \wedge \left(\{D\} = 1 = max(\{k,1\})\right)$

(2) $(k = 0) \implies \left(\exists_{\mathcal{D}}\left(\left(\forall_{D \in \mathcal{D}}(Trail[D,G])\right) \wedge (Decomposition[\mathcal{D},G]) \wedge \left(|\mathcal{D}| = max(\{k,1\})\right)\right)\right)$

(3) $(k > 0) \implies \ldots$

(3.1) Since each trail adds an even degree to each non-endpoint vertex, we need at least k trails to partition the $2k$ odd vertices.

(3.2) Partition the edges into k trails such that the ends of each trail will land on an odd vertex.

(3.3) Construct a new graph G' where the k trails are connected by an edge. ▮ $\left(\exists!_{H' \in \mathcal{H}'}(\neg Trivial[H'])\right) \wedge (EvenGraph[G'])$

(3.4) $EulerianEquiv$ ▮ $Eulerian[G']$ ▮ $\exists_{W'}(EulerianCircuit[W',G'])$

(3.5) Construct $\mathcal{D}$ to be the trails in W' separated by $E(G) \setminus E(G')$. ▮ $(Decomposition[\mathcal{D},G]) \wedge (\mathcal{D} = k))$

(4) $(k > 0) \implies \left(\exists_{\mathcal{D}}\left(\left(\forall_{D \in \mathcal{D}}(Trail[D,G])\right) \wedge (Decomposition[\mathcal{D},G]) \wedge \left(|\mathcal{D}| = max(\{k,1\})\right)\right)\right)$

(5) $\exists_{\mathcal{D}}\left(\left(\forall_{D \in \mathcal{D}}(Trail[D,G])\right) \wedge (Decomposition[\mathcal{D},G]) \wedge \left(|\mathcal{D}| = max(\{k,1\})\right)\right)$

1.1.4 Vertex Degrees and Counting

$MinDegree[\delta(G),G] := \delta(G) = min\left(\{d(v) \mid v \in V(G)\}\right)$
$MinDegree[\Delta(G),G] := \Delta(G) = max\left(\{d(v) \mid v \in V(G)\}\right)$
$RegularG[G] := \delta(G) = \Delta(G)$
$kRegularG[G,k] := k = \delta(G) = \Delta(G)$
$Neighborhood[N(v),v,G] := N(v) = \{u \in V(G) \mid AdjacentV[\{u,v\},G]\}$

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

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

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

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

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

(1) $DegreeSumFormula$ ▮ $Even\left(\sum_{v \in V(G)} \big(d(v)\big)\right)$

(2) $\Big(Odd\Big(|\{v \in V(G) \mid Odd\big(d(v)\big)\}|\Big)\Big) \implies \left(Odd\left(\sum_{v \in V(G)} \big(d(v)\big)\right)\right) \implies (\bot)$ ▮ $Even\Big(|\{v \in V(G) \mid Odd\big(d(v)\big)\}|\Big)$

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

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

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

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

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

1.1.5 Trees

$Acyclic[G] := \neg\exists_C\big((Subgraph[C,G]) \wedge (CycleG[C])\big)$
$Forest[G] := Acyclic[G]$
$Tree[G] := (Connected[G]) \wedge (Acyclic[G])$
$Leaf[v,G] := d(v) = 1$
$SpanningSubgraph[H,G] := (Subgraph[H,G]) \wedge \big(V(H) = V(G)\big)$
$SpanningTree[H,G] := (SpanningSubgraph[H,G]) \wedge (Tree[G])$

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

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

(2) $\big(2 \leq n(G)\big) \wedge (Connected[G])$ ▮ $\exists_e\big(e \in E(G)\big)$ ▮ Let P be the maximal path of e.

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

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

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

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

(3) Since deleting a vertex cannot create a cycle. ▮ $Acyclic[G - v]$

(4) $Tree[G - v]$

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

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

(1.1) $Tree[G]$ ▮ $Connected[G]$

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

(1.3) $\left((n > 1) \wedge \left(\forall_{G'}\left(\Big(\big(n(G') < n\big) \wedge (Tree[G'])\Big) \implies \big(e(G') = n(G') - 1\big)\right)\right)\right) \implies \ldots$

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

(1.3.2) $Leaf\,Deletion \blacksquare Tree[G-v]$

(1.3.3) By IH, $e(G-v) = (n-1)-1 = n-2$

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

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

(1.5) By induction, $e(G) = n-1 \blacksquare (Connected[G]) \wedge \left(e(G) = n-1\right)$

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

(3) $\left((Connected[G]) \wedge \left(e(G) = n-1\right)\right) \implies \ldots [B \implies C]$

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

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

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

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

(3.5) $(Acyclic[G]) \wedge \left(e(G) = n-1\right)$

(4) $\left((Connected[G]) \wedge \left(e(G) = n-1\right)\right) \implies \left((Acyclic[G]) \wedge \left(e(G) = n-1\right)\right)$

(5) $\left((Acyclic[G]) \wedge \left(e(G) = n-1\right)\right) \implies \ldots [C \implies A]$

(5.1) $Acyclic[G]$

(5.2) $Components[\langle G_i \rangle_{i=1}^{k}, G] \blacksquare \sum_{i=1}^{k}\left(n(G_i)\right) = n(G) = n$

(5.3) $\forall_{i \in \mathbb{N}_1^k}(Component[G_i, G]) \blacksquare \forall_{i \in \mathbb{N}_1^k}(Connected[G_i])$

(5.4) $\forall_{i \in \mathbb{N}_1^k}\left((Connected[G_i]) \wedge (Acyclic[G_i])\right)$

(5.5) $([A \implies B]) \wedge \left(\forall_{i \in \mathbb{N}_1^k}\left((Connected[G_i]) \wedge (Acyclic[G_i])\right)\right) \blacksquare \forall_{i \in \mathbb{N}_1^k}\left(e(G_i) = n(G_i)-1\right)$

(5.6) $e(G) = \sum_{i=1}^{k}\left(e(G_i)\right) = \sum_{i=1}^{k}\left(n(G_i)-1\right) = n-k$

(5.7) $\left(e(G) = n-k\right) \wedge \left(e(G) = n-1\right) \blacksquare k = 1 \blacksquare Connected[G]$

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

(6) $\left((Acyclic[G]) \wedge \left(e(G) = n-1\right)\right) \implies (Tree[G])$

(7) $(Tree[G]) \implies \ldots [A \implies D]$

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

(7.2) $Connected[G] \blacksquare \forall_{u,v \in V(G)} \exists_P \left(uvPath[(u,v), P]\right)$

(7.3) $\left(\left(u, v \in V(G)\right) \wedge \left(uvPath[(u,v), P_1]\right) \wedge \left(uvPath[(u,v), P_2]\right)\right) \implies \ldots$

(7.3.1) $(P_1 \neq P_2) \implies \ldots$

(7.3.1.1) Take the shortest subpaths P_1', P_2' of P_1, P_2 that ends on the same endpoints u', v'.

(7.3.1.2) By the extremal choice, P_1', P_2' share the same endpoints, but no internal vertices. $\blacksquare Cycle[P_1' \cup P_2']$

(7.3.1.3) $(Acyclic[G]) \wedge (Cycle[P_1' \cup P_2']) \blacksquare \perp$

(7.3.2) $(P_1 \neq P_2) \implies (\perp) \blacksquare P_1 = P_2$

(7.4) $\left(\left(u, v \in V(G)\right) \wedge \left(uvPath[(u,v), P_1]\right) \wedge \left(uvPath[(u,v), P_2]\right)\right) \implies (P_1 = P_2)$

(8) $(Tree[G]) \implies \left(\forall_{u,v \in V(G)} \exists!_P \left(uvPath[(u,v), P]\right)\right)$

(9) $\left(\forall_{u,v \in V(G)} \exists!_P \left(uvPath[(u,v), P]\right)\right) \implies \ldots [D \implies A]$

(9.1) $\forall_{u,v \in V(G)} \exists!_P \left(uvPath[(u,v), P]\right) \blacksquare \forall_{u,v \in V(G)} \exists_P \left(uvPath[(u,v), P]\right) \blacksquare Connected[G]$

(9.2) $(\neg Acyclic[G]) \implies \ldots$

(9.2.1) $\exists_C \left(Cycle[C] \wedge (Subgraph[C, G])\right)$

(9.2.2) $\forall_{c_1, c_2 \in C} \exists_{P,P'} \left((P \neq P') \wedge \left(uvPath[(c_1, c_2), P]\right) \wedge \left(uvPath[(c_1, c_2), P']\right)\right)$

(9.2.3) $\left(\forall_{u,v\in V(G)}\exists!_P\left(uvPath[(u,v),P]\right)\right)\wedge\left(\forall_{c_1,c_2\in C}\exists_{P,P'}\left((P\neq P')\wedge\left(uvPath[(c_1,c_2),P]\right)\wedge\left(uvPath[(c_1,c_2),P']\right)\right)\right) \blacksquare \perp$

(9.3) $(\neg Acyclic[G]) \implies (\perp) \blacksquare Acyclic[G]$

(9.4) $(Connected[G])\wedge(Acyclic[G])$

(10) $\left(\forall_{u,v\in V(G)}\exists!_P\left(uvPath[(u,v),P]\right)\right) \implies (Tree[G])$

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

(1) $(Tree[G]) \implies \ldots [A]$

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

(1.2) $TreeEquiv \blacksquare \forall_{u,v\in V(G)}\exists!_P\left(uvPath[(u,v),P]\right) \blacksquare \forall_{\{u,v\}\in E(G)}(CutEdge[\{u,v\},G])$

(2) $(Tree[G]) \implies \left(\forall_{e\in E(G)}(CutEdge[e,G])\right)$

(3) $(Tree[G]) \implies \ldots [B]$

(3.1) $Tree[G] \blacksquare Connected[G]$

(3.2) $TreeEquiv \blacksquare \forall_{u,v\in V(G)}\exists!_P\left(uvPath[(u,v),P]\right) \blacksquare \exists!_C\left((Cycle[C])\wedge(Subgraph[C,G+e])\right)$

(4) $(Tree[G]) \implies \left(\exists!_C\left((Cycle[C])\wedge(Subgraph[C,G+e])\right)\right)$

(5) $(Connected[G]) \implies \ldots [C]$

(5.1) Delete all edges that form a cycle in G to form G'. $\blacksquare (Acyclic[G'])\wedge\left(V(G')=V(G)\right)$

(5.2) $V(G')=V(G) \blacksquare SpanningSubgraph[G',G]$

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

(5.4) $(Connected[G'])\wedge(Acyclic[G']) \blacksquare Tree[G']$

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

(6) $(Connected[G]) \implies \left(\exists_T(SpanningTree[T,G])\right)$

CONTHERE p. 69

$$Walk[W,G] := \left(\forall_{i\in\mathbb{N}_1^{|W|}}\left(w_i \in V(G)\right)\right) \wedge \left(\forall_{i\in\mathbb{N}_1^{|W|-1}}\left(\{v_i, v_{i+1}\} \in E(G)\right)\right)$$
$$WalkEV[(x,y),(W,G)] := (Walk[W,G]) \wedge (x,y) = (w_1, w_{|W|})$$
$$WalkL[l,(W,G)] := (Walk[W,G]) \wedge (l = |W| - 1)$$
$$TrailW[W,G] := (Walk[W,G]) \wedge \left(\forall_{i,j\in\mathbb{N}_1^{|W|-1}}\left((i \neq j) \implies (\{w_i, w_{i+1}\} \neq \{w_j, w_{j+1}\})\right)\right)$$
$$PathW[W,G] := (Walk[W,G]) \wedge \left(\forall_{i,j\in\mathbb{N}_1^{|W|}}\left((i \neq j) \implies (w_i \neq w_j)\right)\right)$$

$$ClosedWalk[W,G] := (Walk[W,G]) \wedge (w_{|W|} = w_1)$$
$$Circuit[W,G] := (Trail[W,G]) \wedge (ClosedWalk[W,G])$$
$$CycleW[W,G] := (ClosedWalk[W,G]) \wedge \left(\forall_{i\in\mathbb{N}_2^{|W|-1}}(w_0 \neq w_i \neq w_{|W|})\right) \wedge \left(\forall_{i,j\in\mathbb{N}_2^{|W|-1}}\left((i \neq j) \implies (w_i \neq w_j)\right)\right) \wedge (|W| - 1 \geq 3)$$
$$CycleE[E,(W,G)] := (CycleW[W,G]) \wedge (E = \{\{w_i, w_{i+1}\} \mid i \in \mathbb{N}_1^{|W|-1}\})$$
$$EvenCycleW[W,G] := (CycleW[W,G]) \wedge \left(Even(|W| - 1)\right)$$
$$OddCycleW[W,G] := (CycleW[W,G]) \wedge \left(Odd(|W| - 1)\right)$$
$$TriangleW[W,G] := (CycleW[W,G]) \wedge (|W| - 1 = 3)$$

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

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

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

---

(1) $\left(\exists_{\mathcal{C}}\left(\left(\mathcal{E} = \{C_E \mid (C \in \mathcal{C}) \wedge \left(CycleE[C_E,(C,G)]\right)\}\right) \wedge \left(Partition[\mathcal{E}, E(G)]\right)\right)\right) \implies \ldots$

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

---

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

---

(3) $\left(\forall_{v\in V(G)}\left(Even\left(d(v)\right)\right)\right) \implies \ldots$

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

(3.2) $\left(e(G) \neq 0\right) \implies \ldots$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1.6) $\left(2e(G)\right)^2 \leq n^2\left(e(G)\right) \;\blacksquare\; e(G) \leq n^2/4$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chapter 2

Abstract Algebra

2.1 Functions

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

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

(1) TODO

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

(1) TODO

$Domain[dom(f), f, X, Y] := (Func[f, X, Y]) \wedge \big(dom(f) = X\big)$
$Codomain[cod(f), f, X, Y] := (Func[f, X, Y]) \wedge \big(cod(f) = Y\big)$
$Image[im(A), A, f, X, Y] := (Func[f, X, Y]) \wedge (A \subseteq X) \wedge \big(im(A) = \{f(a) \in Y \mid a \in A\}\big)$
$Preimage[pim(B), B, f, X, Y] := (Func[f, X, Y]) \wedge (B \subseteq Y) \wedge \big(pim(B) = \{a \in X \mid f(a) \in B\}\big)$
$Range[rng(f), f, X, Y] := (Func[f, X, Y]) \wedge \big(Image[rng(f), dom(f), f, X, Y]\big)$

$Inj[f, X, Y] := (Func[f, X, Y]) \wedge \left(\forall_{x_1, x_2 \in X}\left(\big(f(x_1) = f(x_2)\big) \implies (x_1 = x_2)\right)\right)$
$Surj[f, X, Y] := (Func[f, X, Y]) \wedge \left(\forall_{y \in Y} \exists_{x \in X} \big(y = f(x)\big)\right)$
$Bij[f, X, Y] := (Inj[f, X, Y]) \wedge (Surj[f, X, Y])$
$Inv[f^{-1}, f, X, Y] := (Func[f, X, Y]) \wedge (Func[f^{-1}, Y, X]) \wedge (f \circ f^{-1} = I_Y) \wedge (f^{-1} \circ f = I_X)$

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

(1) TODO

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

(1) TODO

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

(1) TODO

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

(1) TODO

2.2 Divisibility, Equivalence Relations, Paritions

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

(1) TODO

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

$$Partition[\mathcal{P}, S] := \big(\forall_{P\in\mathcal{P}}(P \neq \emptyset)\big) \wedge \left(S = \bigcup_{P\in\mathcal{P}}(P)\right) \wedge \Big(\forall_{P_1,P_2\in\mathcal{P}}\big((P_1 \neq P_2) \implies (P_1 \cap P_2 = \emptyset)\big)\Big)$$
$$EqRel[\sim, S] := (Rel[\sim, S]) \wedge \big(\forall_{a\in S}(a \sim a)\big) \wedge \Big(\forall_{a,b\in S}\big((a \sim b) \implies (b \sim a)\big)\Big) \wedge \Big(\forall_{a,b,c\in S}\Big(\big((a \sim b) \wedge (b \sim c)\big) \implies (a \sim c)\Big)\Big)$$
$$EqClass[[s], s, \sim, S] := (Rel[\sim, S]) \wedge (s \in S) \wedge ([s] = \{x \in S \mid x \sim s\})$$

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

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

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

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

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

(1) TODO

2.3 Groups

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

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

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

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

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

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

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

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

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

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

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

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

(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

$Subgroup[H, G, *] := (Group[G,*]) \wedge (H \subseteq G) \wedge (Group[H,*])$
$TrivSubgroup[H, G, *] := (H = \{e\}) \vee (H = G)$
$PropSubgroup[H, G, *] := (Subgroup[H, G, *]) \wedge (\neg TrivSubgroup[H, G, *])$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(5) $\big(a \in C(g)\big) \implies \ldots$

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

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

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

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

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

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

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

2.5 Special Groups

2.5.1 Cyclic Group

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.6 Lagrange's Theorem

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.7 Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) $OrderElDivOrder$ ▌ $g^n = e_G$

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

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

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

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

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

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

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

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

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

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

(2) $(g_1, g_2 \in G) \implies \ldots$

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

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

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

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

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

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

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

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

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

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

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

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

(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) $\ldots (Func[\phi, G, H]) \wedge (Inj[\phi, G, H]) \wedge (Surj[\phi, G, H]]) \;\blacksquare\; Bij[\phi, G, H]$

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

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

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

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

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

2.8 Kernel and Image Homomorphisms

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

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

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

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

(2) $ker_\phi \subseteq G \;\blacksquare\; \emptyset \neq ker_\phi \subseteq G$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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) $\Big(x\in(ker_\phi)g\Big) \implies \dots$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(7) ==

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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) $SubgroupCenter \blacksquare Subgroup[Z(G), G, *]$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.11 Quotient Groups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(7) $...(Func[\psi, G/ker_\phi, im_\phi]) \wedge (Inj[\psi, G/ker_\phi, im_\phi]) \wedge (Surj[\psi, G/ker_\phi, im_\phi]) \blacksquare \; Bij[\psi, G/ker_\phi, im_\phi]$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(9) $\left((n \in N) \wedge (h_1 n_1 \in HN)\right) \implies ...$

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

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

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

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

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

(14) $\left((x \in H \cap N) \wedge (h \in H)\right) \implies ...$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$ThirdIsoThm := \begin{pmatrix} \big((NormalSubgroup[K, G, *]) \wedge (NormalSubgroup[H, G, *]) \wedge (Subgroup[K, H, *])\big) \implies \\ \big(Isomorphic[(G/K)/(H/K), \bar{*}, G/H, \bar{*}]\big) \end{pmatrix}$$

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

(2) $\Big(\big(g_1K, g_2K \in (G/K)\big) \wedge (g_1K = g_2K)\Big) \implies \ldots$

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

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

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

(3) $\Big(\big(g_1K, g_2K \in (G/K)\big) \wedge (g_1K = g_2K)\Big) \implies \big(\phi(g_1K) = \phi(g_2K)\big)$ ▮ $\forall_{g_1K, g_2K \in (G/K)}\Big((g_1K = g_2K) \implies \big(\phi(g_1K) = \phi(g_2K)\big)\Big) \ldots$

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

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

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

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

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

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

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

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

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

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