Contents

Chapter 1

Graph Theory

1.1 Graphs

1.1.1 **Graph operations**

$GraphPower[G^r, r, G] := (V = V(G)) \wedge (E = \{\{x, y\} \mid d(x, y) \leq r\}) \wedge (G^r = (V, E))$
$GraphSum[G_1 + G_2, G_1, G_2] := (V = V(G_1) \cup V(G_2)) \wedge (E = E(G_1) \cup E(G_2) \cup \{\{x, y\} \mid (x \in V(G_1)) \wedge y \in V(G_2)\}) \wedge (G_1 + G_2 = (V, E))$

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

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

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

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

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

---

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

1.1.2 Graphs

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

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

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

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

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

1.1.3 Paths, Cycles, Trails

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

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

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

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

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

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

(1) Bijection and composition properties

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

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

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

TODO: ADD SPECIAL GRAPHS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) Starting from $E(G) = \emptyset$, $|\mathcal{H}| = n$

(2) Adding an edge would decrease the number of components by 0 or 1, so after adding k edges, $n - k \leq |\mathcal{H}|$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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 $\exists_{C'}((WalkContainsCycle[C', W_1, G]) \wedge (Odd(e(C'))))$

(2.2.3) $\exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C))))$

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

(2.4) $\exists_C((WalkContainsCycle[C, W, G]) \wedge (Odd(e(C))))$

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

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

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

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

(1) $(Bipartite[G]) \implies \ldots$

(1.1) Every step alternates between each bipartition. Thus the end vertex of the odd walk cannot be the start vertex, and it is not a cycle.

(1.2) $\neg\exists_C((CycleG[C]) \wedge (Subgraph[C, G]) \wedge (Odd(e(C))))$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1.2.2) $(BipartiteG[K_1]) \wedge (BipartiteG[K_2]) \blacksquare Bipartite[K_n]$

(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 $\blacksquare$ $\neg Bipartite[K_n]$ $\blacksquare$ $\bot$

(1.4.2) $(n > 2) \implies (\bot)$ $\blacksquare$ $n \leq 2$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$MaximalPath[P, G] := (Subgraph[P, G]) \wedge (PathG[P]) \wedge (\neg\exists_{P'\neq P}((Subgraph[P, P']) \wedge (Subgraph[P', G]) \wedge (PathG[P'])))$
$MaximalTrail[W, G] := (Trail[W, G]) \wedge (\neg\exists_{W'\neq W}((W \subseteq W') \wedge (Trail[W', G])))$

$VertexDegreeCycle := (\forall_{v\in V(G)}(2 \leq d(v))) \implies (\exists_C((Subgraph[C, G]) \wedge (CycleG[C])))$

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

(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. $\exists_C((Subgraph[C, G]) \wedge (CycleG[C]))$.

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

(1) $(Eulerian[G]) \implies \ldots$

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

(1.2) The first and last vertices have even degree, and the intermediate vertices have even degree. ▮ $EvenGraph[G]$

(1.3) $E(G)$ must be covered by the W, thus they must lie on the same non-trivial component. ▮ $(\nexists \vee \exists!)_{H \in \mathcal{H}}(\neg Trivial[H])$

(1.4) $((\nexists \vee \exists!)_{H \in \mathcal{H}}(\neg Trivial[H])) \wedge (EvenGraph[G])$

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

(3) $(((\nexists \vee \exists!)_{H \in \mathcal{H}}(\neg Trivial[H])) \wedge (EvenGraph[G])) \implies \ldots$

(3.1) $(E(G) = 0) \implies \ldots$

(3.1.1) Let the Eulerian circuit be consist of just one vertex. ▮ $Eulerian[G]$

(3.2) $(E(G) = 0) \implies (Eulerian[G])$

(3.3) $((E(G) > 0) \wedge (\forall_{G'}((E(G') < E(G)) \implies (Eulerian[G'])))) \implies \ldots$

(3.3.1) $\exists!_H(H \in \mathcal{H} \mid \neg Trivial[H])$

(3.3.2) $EvenGraph[G]$ ▮ $EvenGraph[H]$ ▮ $\forall_{v \in V(H)}(2 \leq d(v))$

(3.3.3) $VertexDegreeCycle$ ▮ $\exists_C((Subgraph[C, H]) \wedge (CycleG[C]))$

(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 $\forall_{H' \in \mathcal{H}'}(E(H') < E(G))$ ▮ $\forall_{H' \in \mathcal{H}'}(Eulerian[H'])$

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

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

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

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

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

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

(2.1) $(E(G) > 0) \wedge (EvenGraph[G])$ ▮ $\forall_{v \in V(G)}(2 \leq d(v))$

(2.2) $VertexDegreeCycle$ ▮ $\exists_C((Subgraph[C, G]) \wedge (CycleG[C]))$

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

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

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

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

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

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

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

(4) Thus P has at least k vertices. ▮ $k \leq E(P)$.

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

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

(1) $VertexDegreePathk$ ▮ $\exists_P((Subgraph[P, G]) \wedge (PathG[P]) \wedge (k \leq e(P)))$

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

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

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

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

(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'. ▌ $\neg CutVertex[u',G]$

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

(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. ▌ $ClosedWalk[W,G]$

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

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

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

(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. ▌ $(\exists!_{H' \in \mathcal{H}'}(\neg Trivial[H'])) \wedge (EvenGraph[G'])$

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

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

1.1.4 Vertex Degrees and Counting

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

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

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

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

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

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

(1) $DegreeSumFormula$ ▌ $Even(\sum_{v \in V(G)}(d(v)))$

(2) $(Odd(|\{v \in V(G) \mid Odd(d(v))\}|)) \implies (Odd(\sum_{v\in V(G)}(d(v)))) \implies (\perp)$ ▌ $Even(|\{v \in V(G) \mid Odd(d(v))\}|)$

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

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

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

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

(1) $kRegularG[G,k]$ ▌ $(e(G) = 2|X|) \land (e(G) = 2|Y|)$ ▌ $|X| = |Y|$

1.1.5 Trees

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

$LeafExistence := ((Tree[G]) \land (2 \le n(G))) \implies (2 \le |\{v \in V(G) \mid Leaf[v,G]\}|)$

(1) $Tree[G]$ ▌ $(Connected[G]) \land (Acyclic[G])$

(2) $(2 \le n(G)) \land (Connected[G])$ ▌ $\exists_e(e \in E(G))$ ▌ Let P be the maximal path of e.

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

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

(1) $Tree[G]$ ▌ $(Connected[G]) \land (Acyclic[G])$

(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) $Tree[G-v]$

$$TreeEquiv := (n = n(G) \ge 1) \implies \begin{pmatrix} (A) & (Tree[G]) & \iff \\ (B) & ((Connected[G]) \land (e(G) = n-1)) & \iff \\ (C) & ((Acyclic[G]) \land (e(G) = n-1)) & \iff \\ (D) & (\forall_{u,v\in V(G)}\exists!_P(uvPath[(u,v),P])) & \end{pmatrix}$$

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

(1.1) $Tree[G]$ ▌ $Connected[G]$

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

(1.3) $((n > 1) \land (\forall_{G'}(((n(G') < n) \land (Tree[G'])) \implies (e(G') = n(G') - 1)))) \implies \dots$

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

(1.3.2) $LeafDeletion$ ▌ $Tree[G-v]$

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

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

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

(1.5) By induction, $e(G) = n-1$ ▌ $(Connected[G]) \land (e(G) = n-1)$

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

(3) $((Connected[G]) \land (e(G) = n-1)) \implies \dots [B \implies C]$

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

(3.2) $(Connected[G]) \land (CutEdgeEquiv)$ ▌ $Connected[G']$

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

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

(3.5) Equivalently, $G' = G - E = G - \emptyset = G$ ▮ $G = G'$

(3.6) $(Acyclic[G]) \wedge (e(G) = n - 1)$

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

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

(5.1) $Acyclic[G]$

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

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

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

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

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

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

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

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

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

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

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

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

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

(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. ▮ $Cycle[P_1' \cup P_2']$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1.1) $Tree[G]$ ▮ $Connected[G]$

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

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

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

(3.1) $Tree[G]$ ▮ $Connected[G]$

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

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

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

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

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

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

CONTHERE p. 69

Chapter 2

Abstract Algebra

2.1 Functions

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

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

(1) TODO

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

(1) TODO

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

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

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

(1) TODO

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

(1) TODO

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

(1) TODO

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

(1) TODO

2.2 Divisibility, Equivalence Relations, Paritions

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

(1) TODO

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

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

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

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

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

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

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

(1) TODO

2.3 Groups

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

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

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

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

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

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

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

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

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

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

2.4 Subgroups

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

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

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

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

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

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

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

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

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

(2.6) $Group[H, *]$

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

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

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

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

(1) TODO

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

(1) $Group[G, *]$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5 Special Groups

2.5.1 Cyclic Group

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5.2 Symmetric and Alternating Groups

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

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

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

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

2.5.3 Dihedral Group

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

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

2.6 Lagrange's Theorem

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) $LagrangeTheorem$ $\blacksquare$ 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

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

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

2.7 Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3.2) $...\ (\phi(g^{n_1}) = \phi(g^{n_2}))$ ▌ $(g^{n_1} = g^{n_2}) \iff (\phi(g^{n_1}) = \phi(g^{n_2}))$

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

(5) $...\ (Func[\phi, G, H]) \wedge (Inj[\phi, G, H]) \wedge (Surj[\phi, G, H]])$ ▌ $Bij[\phi, G, H]$

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

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

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

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

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

2.8 Kernel and Image Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3.1) $((g_1, g_2 \in G) \land (\phi(g_1) = \phi(g_2))) \implies \ldots$

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

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

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

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

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

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

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

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

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

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

(3) $((x \in G) \land (\phi(x) = \phi(g))) \implies \ldots$

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

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

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

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

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

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

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

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

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

(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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(7) ==

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.10 Normal Subgroups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.11 Quotient Groups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) $(h_1n_1, h_2n_2 \in HN) \implies \ldots$

(3.1) $h_2 \in G \blacksquare (h_2)^{-1}n_1h_2 \in N$

(3.2) $(h_1n_1)(h_2n_2) = h_1(h_2(h_2)^{-1})n_1h_2n_2 = (h_1h_2)((h_2)^{-1}n_1h_2n_2) \blacksquare (h_1n_1)(h_2n_2) = (h_1h_2)((h_2)^{-1}n_1h_2n_2)$

(3.3) $(Group[H, *]) \wedge (Group[N, *]) \blacksquare (h_1h_2 \in H) \wedge ((h_2)^{-1}n_1h_2n_2 \in N)$

(3.4) $(h_1n_1)(h_2n_2) = (h_1h_2)((h_2)^{-1}n_1h_2n_2 \in N \blacksquare (h_1n_1)(h_2n_2) \in N$

(4) $(h_1n_1, h_2n_2 \in HN) \implies ((h_1n_1)(h_2n_2) \in N) \blacksquare \forall_{h_1n_1, h_2n_2 \in HN}((h_1n_1)(h_2n_2) \in N)$

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

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

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

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

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

(7) $(\emptyset \neq HN \subseteq G) \wedge (\forall_{h_1n_1, h_2n_2 \in HN}((h_1n_1)(h_2n_2) \in N)) \wedge (\forall_{hn \in HN}((hn)^{-1} \in HN)) \blacksquare Subgroup[HN, G, *] \blacksquare Group[HN, *]$

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

(9) $((n \in N) \wedge (h_1n_1 \in HN)) \implies \ldots$

(9.1) $(NormalSubgroup[N, G, *]) \wedge (h_1n_1 \in G) \blacksquare (h_1n_1)^{-1}n(h_1n_1) \in N$

(10) $((n \in N) \wedge (h_1n_1 \in HN)) \implies ((h_1n_1)^{-1}n(h_1n_1) \in N) \blacksquare \forall_{n \in N}\forall_{h_1n_1 \in HN}((h_1n_1)^{-1}n(h_1n_1) \in N)$

(11) $(Subgroup[N, HN, *]) \wedge (\forall_{n \in N}\forall_{h_1n_1 \in HN}((h_1n_1)^{-1}n(h_1n_1) \in N)) \blacksquare NormalSubgroup[N, HN, *]$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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) $((g_1K, g_2K \in (G/K)) \wedge (g_1K = g_2K)) \implies (\phi(g_1K) = \phi(g_2K))$ ▮ $\forall_{g_1K,g_2K \in (G/K)}((g_1K = g_2K) \implies (\phi(g_1K) = \phi(g_2K)))$ . . .

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

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

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

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

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

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

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

(9.2) $g \in G$ ▮ $gK \in (G/K)$

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

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

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

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

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

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