Contents

Chapter 1

Graph Theory

1.1 Graphs

$Graph[(V,E)] := (V \cap E = \emptyset) \wedge (E \subseteq V^{\{2\}})$

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

$VertexSet[V((V,E)),(V,E)] := \big(Graph[(V,E)]\big) \wedge \Big(V\big((V,E)\big) = V\Big)$

$EdgeSet[E((V,E)),(V,E)] := \big(Graph[(V,E)]\big) \wedge \Big(E\big((V,E)\big) = E\Big)$

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

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

$AdjacentE[(a,b),G] := \exists!_{x \in V(G)}\big((x \in a) \wedge (x \in b)\big)$

$\boxed{[\text{Notation}] \quad x\,y := AdjacentV[(x,y),G]}$

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

$SubgraphInducedByV[G[V'],V',G] := \big(E' = \{e \in E(G) \mid \exists_{a,b \in V'}(Incident[e,a,b,G])\}\big) \wedge \big(G[V'] = (V',E')\big)$

$InducedSubgraph[H,G] := (Subgraph[H,G]) \wedge (SpannedBy[H,V(H),G])$

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

$RemoveV[G-W,W,G] := \big(W \subseteq V(G)\big) \wedge \big(SubgraphInducedByV[G-W,V(G) \setminus W,G]\big)$

$RemoveE[G-E,E,G] := \big(E \subseteq E(G)\big) \wedge \Big(G-E = (V(G),E(G) \setminus E)\Big)$

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

$EvenCycle[W, G] := (Cycle[W, G]) \wedge \left(Even(|W| - 1)\right)$

$OddCycle[W, G] := (Cycle[W, G]) \wedge \left(Odd(|W| - 1)\right)$

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

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

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

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

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

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

$CycleG[C_n, n] := \left(V(C_n) = V(P_n)\right) \wedge \left(E(C_n) = E(P_n) \cup \{\{x_n, x_1\}\}\right)$

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

---

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

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

---

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

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

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

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

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

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

(3.2.3) $(d_G(x_0) \geq 2)$ ▊ Let y be another vertex adjacent to x_0 that is not x_1.

(3.2.4) If y is not in P, then P is not a maximal PathG - contradiction.

(3.2.5) Thus y is in P, and P contains a cycle C.

(3.2.6) Let $G' = G - E(C)$. ▊ $\left(\forall_{v \in V(G')} \left(Even(d_{G'}(v)) \right) \right)$ ▊ Repeat on G' until all disjoint cycles C are found.

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

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

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

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

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

p. 21

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

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

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

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

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

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

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

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

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

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

(1) SumDeg

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

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

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

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

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

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

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

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

(1)   TODO $\phi = \ldots$

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

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

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

(2)   By cases:

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

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

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

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

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

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

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

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

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

$KroneckerProperties := \ldots$

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

---

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

(1)   TODO

---

acyclic graph

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

forest -> decomponents into trees

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

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

(1) TODO

(1) TODO

Chapter 2

Abstract Algebra

2.1 Functions

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

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

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

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

(1) TODO

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

(1) TODO

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

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

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

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

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

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

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

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

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

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

(1) TODO

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

(1) TODO

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

(1) TODO

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

(1) TODO

2.2 Divisibility, Equivalence Relations, Paritions

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

(1)   TODO

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

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

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

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

(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

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

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

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

---

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

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

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

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

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

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

   (3.1)   TODO

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

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

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

---

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

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

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

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

(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

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

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

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

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

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

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

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

(1)	$e * g = g * e \ \blacksquare\ e \in C(g) \ \blacksquare\ C(g) \neq \emptyset$
(2)	$C(g) \subseteq G \ \blacksquare\ \emptyset \neq C(g) \subseteq G$
(3)	$\left(a, b \in C(g) \right) \implies \ldots$
(3.1)	$(a * g = g * a) \wedge (b * g = g * b)$
(3.2)	$(a * b) * g = a * (b * g) = a * (g * b) = (a * g) * b = (g * a) * b = g * (a * b) \ \blacksquare\ a * b \in C(g)$
(4)	$\left(a, b \in C(g) \right) \implies \left(a * b \in C(g) \right) \ \blacksquare\ \forall_{a, b \in C(g)} \left(a * b \in C(g) \right)$
(5)	$\left(a \in C(g) \right) \implies \ldots$
(5.1)	$a * g = g * a$
(5.2)	$a^{-1} * (a * g) * a^{-1} = a^{-1} * (g * a) * a^{-1} \ \blacksquare\ g * a^{-1} = a^{-1} * g \ \blacksquare\ a^{-1} \in C(g)$
(6)	$\left(a \in C(g) \right) \implies \left(a^{-1} \in C(g) \right) \ \blacksquare\ \forall_{a \in C(g)} \left(a^{-1} \in C(g) \right)$
(7)	$(SubgroupEquiv) \wedge \left(\emptyset \neq C(g) \subseteq G \right) \wedge \left(\forall_{a, b \in C(g)} \left(a * b \in C(g) \right) \right) \wedge \left(\forall_{a \in C(g)} \left(a^{-1} \in C(g) \right) \right) \ \blacksquare\ Subgroup[C(g), G, *]$

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

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

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

2.5 Special Groups

2.5.1 Cyclic Group

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

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

(1)	$\exists_{g \in G} (Generator[g, G, *])$
(2)	$H \subseteq G \ \blacksquare\ \exists_{m \in \mathbb{Z}^+} \left((g^m \in H) \wedge \left(\forall_{k \in \mathbb{Z}^+} ((k < m) \implies (g^k \notin H)) \right) \right)$
(3)	$(b \in H) \implies \ldots$
(3.1)	$H \subseteq G \ \blacksquare\ \exists_{n \in \mathbb{Z}^+} (b = g^n)$
(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)	$g^n = g^{mq+r} = g^{mq} * g^r$ ▮ $g^r = (g^{mq})^{-1} * g^n$
(3.4)	$g^n, g^m \in H$ ▮ $g^n, (g^{mq})^{-1} \in H$ ▮ $g^r = g^{mq})^{-1} * g^n \in H$ ▮ $g^r \in H$
(3.5)	$(g^r \in H) \wedge (0 \leq r < m) \wedge \left(\forall_{k \in \mathbb{Z}^+} \big((k < m) \implies (g^k \notin H) \big) \right)$ ▮ $r = 0$
(3.6)	$(r = 0) \wedge (g^n = g^{mq+r}) \wedge (b = g^n)$ ▮ $b = g^n = g^{mq}$ ▮ $b \in < g^m >$
(4)	$(b \in H) \implies (b \in < g^m >)$ ▮ $H \subseteq < g^m >$
(5)	$(b \in < g^m >) \implies \dots$
(5.1)	$\exists_{k \in \mathbb{Z}} \big(b = (g^m)^k \big)$
(5.2)	$(Group[H, G, *]) \wedge (g^m \in H)$ ▮ $(g^m * g^m \in H) \wedge \left((g^m)^{-1} \in H \right)$
(5.3)	$Induction$ ▮ $b = (g^m)^k \in H$ ▮ $b \in H$
(6)	$(b \in < g^m >) \implies (b \in H)$ ▮ $< g^m > \subseteq H$
(7)	$(H \subseteq < g^m >) \wedge (< g^m > \subseteq H)$ ▮ $H = < g^m >$ ▮ $Generator[g^m, H, *]$ ▮ $\exists_{h \in G}(Generator[h, G, *])$ ▮ $CyclicGroup[H, *]$

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

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

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

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

2.5.2 Symmetric and Alternating Groups

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

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

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

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

2.5.3 Dihedral Group

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

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

2.6   Lagrange's Theorem

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

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

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

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

(1)	$(a, b, c \in G) \implies \ldots$
(1.1)	$(Subgroup[H, G, *]) \implies (e \in H) \implies (a * a^{-1} \in H) \implies (a \sim a)$
(1.2)	$(a \sim b) \implies (a * b^{-1} \in H) \implies \big(b * a^{-1} = (a * b^{-1})^{-1} \in H\big) \implies (b \sim a)$
(1.3)	$\big((a \sim b) \land (b \sim c)\big) \implies (a * b^{-1}, b * c^{-1} \in H) \implies \big(a * c^{-1} = (a * b^{-1}) * (b * c^{-1}) \in H\big)$ ▌ $a \sim c$
(2)	$EqRel[\sim, G]$
(3)	$(a, x \in G) \implies \ldots$
(3.1)	$(x \sim a) \iff (x * a^{-1} \in H) \iff \big(\exists_{h \in H}(x * a^{-1} = h)\big) \iff \big(\exists_{h \in H}(x = h * a)\big) \iff (x \in Ha)$
(4)	$[a] = \{x \in G \mid x \sim a\} = Ha$

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

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

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

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

(1)	$CyclicSubgroup[<g>, g, G, *]$ ▌ $Order[<g>] = m$
(2)	$(LagrangeTheorem) \land (CyclicSubgroup)$ ▌ $Divides[Order[<g>], Order[G]]$ ▌ $Divides[m, n]$
(3)	$g^n = g^{mk} = e^k = e$

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

(1)	$LagrangeTheorem$ ▌ Subgroups must have the order 1 or p ▌ Subgroups are trivial
(2)	CyclicSubgroup of a non-identity element is G ▌ Non-identity elements generates G

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

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

2.7   Homomorphisms

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

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

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

(2) $e_H = \phi(e_G)^{-1} \diamond \phi(e_G) = \phi(e_G)^{-1} \diamond \left(\phi(e_G) \diamond \phi(e_G)\right) = \phi(e_G)$ ▮ $e_H = \phi(e_G)$

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

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

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

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

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

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

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

　(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) $\left(\forall_{m \in \mathbb{N}^+}\left((m \leq n) \implies \left(\phi(g^m) = \phi(g)^m\right)\right)\right) \implies \left(\phi(g^{n+1}) = \phi(g)^{n+1}\right)$

(5) $\left((n = 1) \implies \left(\phi(g^n) = \phi(g)^n\right)\right) \wedge \left(\left(\forall_{m \in \mathbb{N}^+}\left((m \leq n) \implies \left(\phi(g^m) = \phi(g)^m\right)\right)\right) \implies \left(\phi(g^{n+1}) = \phi(g)^{n+1}\right)\right) \ldots$

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

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

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

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

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

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

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

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

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

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

　(2.1) $(Homomorphism[\phi, G, *, H, \diamond]) \wedge (Homomorphism[\theta, H, \diamond, K, \square])$ ▮ $\theta \circ \phi(g_1 * g_2) = \theta\left(\phi(g_1 * g_2)\right) = \ldots$

　(2.2) $\ldots \theta\left(\phi(g_1) \diamond \phi(g_2)\right) = \theta\left(\phi(g_1)\right) \square \theta\left(\phi(g_2)\right) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2)$ ▮ $\theta \circ \phi(g_1 * g_2) = \theta \circ \phi(g_1) \square \theta \circ \phi(g_2)$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.8   Kernel and Image Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.9 Conjugacy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(7) ===

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

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

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

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

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

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

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

   (1.1) $a \in C(g)$ ▮ $ag = ga$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.10   Normal Subgroups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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

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

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

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

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

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

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

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

(1.3) $(Group[H, *]) \wedge (h_1, x h_2 x^{-1} \in H)$ ▌ $h_1 x h_2 x^{-1} \in H$

(1.4) $(h_1 x h_2 x^{-1})(xy) = h_1 x h_2 y = z$ ▌ $(h_1 x h_2 x^{-1})(xy) = z$

(1.5) $(h_1 x h_2 x^{-1} \in H) \wedge \left((h_1 x h_2 x^{-1})(xy) = z \right)$ ▌ $\exists_{h_3 \in H}(z = h_3 xy)$

(2) $\left(\exists_{h_1, h_2 \in H}(z = h_1 x h_2 y) \right) \implies \left(\exists_{h_3 \in H}(z = h_3 xy) \right)$

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

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

(3.2) $Group[H, *]$ ▌ $e \in H$

(3.3) $(e)x(x^{-1}h_3 x)y = h_3 xy = z$ ▌ $(e)x(x^{-1}h_3 x)y = z$

(3.4) $(x^{-1}h_3 x, e \in H) \wedge \left((e)x(x^{-1}h_3 x)y = h_3 xy = z \right)$ ▌ $\exists_{h_1, h_2 \in H}(z = h_1 x h_2 y)$

(4) $\left(\exists_{h_3 \in H}(z = h_3 xy) \right) \implies \left(\exists_{h_1, h_2 \in H}(z = h_1 x h_2 y) \right)$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   (5.1) $\phi(h_1 * h_2) = (h_1 * h_2)N = (h_1 N) \bar{\mp} (h_1 N) = \phi(h_1) \bar{\mp} \phi(h_2)$ ▊ $\phi(h_1 * h_2) = \phi(h_1) \bar{\mp} \phi(h_2)$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   (5.1) $\phi(g_1 K \bar{\mp} g_2 K) = \phi\big((g_1 * g_2)K\big) = (g_1 * g_2)H = (g_1 H) \bar{\mp} (g_2 H) = \phi(g_1 K) \bar{\mp} \phi(g_2 K)$ ▊ $\phi(g_1 K \bar{\mp} g_2 K) = \phi(g_1 K) \bar{\mp} \phi(g_2 K)$

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

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

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

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

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

   (9.2) $g \in G$ ▊ $gK \in (G/K)$

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

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

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

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

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

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