Contents

Chapter 1

Graph Theory

1.1 Graphs

$\mathit{Graph}[(V,E)] := (V \cap E = \emptyset) \wedge (E \subseteq V^{\{2\}})$
$\mathit{SimpleGraph}[(V,E)] := \big(\mathit{Graph}[(V,E)]\big) \wedge (E \subseteq \{\{a,b\} \in V^{\{2\}} \mid a \neq b\})$
$\mathit{VertexSet}[V\big((V,E)\big),(V,E)] := \big(\mathit{Graph}[(V,E)]\big) \wedge \Big(V\big((V,E)\big) = V\Big)$
$\mathit{EdgeSet}[E\big((V,E)\big),(V,E)] := \big(\mathit{Graph}[(V,E)]\big) \wedge \Big(E\big((V,E)\big) = E\Big)$
$\mathit{Adjacent}[x,y,G] := \{x,y\} \in E(G)$
$\mathit{Incident}[e,x,y,G] := e = \{x,y\} \in E(G)$
$\mathit{Order}[|G|,G] := |G| = |V(G)|$
$\mathit{Size}[e(G),G] := e(G) = |E(G)|$

$\mathit{Subgraph}[H,G] := \big(V(H) \subseteq V(G)\big) \wedge \big(E(H) \subseteq E(G)\big)$
$\mathit{SpanningSubgraph}[H,G] := (\mathit{Subgraph}[H,G]) \wedge \big(V(H) = V(G)\big)$
$\mathit{RestrictionV}[G[V'],V',G] := G[V'] = \big(V', \{e \mid \exists_{a,b \in V'}(\mathit{Incident}[e,a,b,G])\}\big)$
$\mathit{InducedSubgraph}[H,G] := (\mathit{Subgraph}[H,G]) \wedge \big(\mathit{RestrictionV}[H,V(H),G]\big)$
$\mathit{RemoveV}[G-v,v,G] := \big(v \in V(G)\big) \wedge \big(\mathit{RestrictionV}[G-v,V(G) \setminus \{v\},G]\big)$
$\mathit{RemoveE}[G-e,e,G] := \big(e \in E(G)\big) \wedge \Big(G-e = \big(V(G),E(G) \setminus \{e\}\big)\Big)$
$\mathit{AddE}[G+e,e,G] := \big(e \notin E(G)\big) \wedge \Big(e \in V(G)^{\{2\}}\Big) \wedge \Big(G+e = \big(V(G),E(G) \cup \{e\}\big)\Big)$
$\mathit{Walk}[V_n,n,G] := \Big(V_n = \{v_i \in V(G) \mid i \in \mathbb{N}_1^{n+1}\}\Big) \wedge \Big(\forall_{i \in \mathbb{N}_1^n}\big(\{v_i,v_{i+1}\} \in E(G)\big)\Big)$
$\mathit{Path}[V_n,n,G] := (\mathit{Walk}[V_n,n,G]) \wedge \Bigg(\forall_{i,j \in \mathbb{N}_1^{n+1}}\Big((i \neq j) \implies (v_i \neq v_j)\Big)\Bigg)$
$\mathit{ClosedWalk}[V_n,n,G] := (\mathit{Walk}[V_n,n,G]) \wedge (v_{n+1} = v_1)$
$\mathit{Cycle}[V_n,n,G] := (\mathit{ClosedWalk}[V_n,n,G]) \wedge (n > 1)$
$\mathit{Triangle}[T,G] := \mathit{Cycle}[T,3,G]$
$\mathit{Girth}[G] := \mathit{min}\Big(\{n \in \mathbb{N} \mid \exists_{V_n}(\mathit{Cycle}[V_n,n,G])\}\Big)$
$\mathit{Circumference}[G] := \mathit{max}\Big(\{n \in \mathbb{N} \mid \exists_{V_n}(\mathit{Cycle}[V_n,n,G])\}\Big)$

$\mathit{ConnectedV}[(x,y),G] := \exists_{n,V_n}\Big((\mathit{Path}[V_n,n,G]) \wedge \big((x,y) = (v_1,v_{n+1})\big)\Big)$
$\mathit{Connected}[G] := \forall_{x,y \in V(G)}\big(\mathit{ConnectedV}[(x,y),G]\big)$
$\mathit{Component}[C,G] := (\mathit{Subgraph}[C,G]) \wedge \Bigg(\forall_{c \in V(C)}\forall_{g \in V(G)}\Big(\big(g \notin V(C)\big) \implies \big(\neg \mathit{ConnectedV}[(g,c),G]\big)\Big)\Bigg)$

$\mathit{Degree}[\mathit{deg}(v),v,G] := \mathit{deg}(v) = |\{e \in E(G) | v \in e\}|$
$\mathit{Regular}[G,r] := \forall_{v \in V(G)}\big(\mathit{deg}(v) = r\big)$

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

---

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

$\mathit{OddDeg} := \mathit{Even}\Big(|\{v \mid \mathit{Odd}\big(\mathit{deg}(v)\big)\}|\Big)$

(1) SumDeg

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

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

$$CycleG[C_n, n] := \left(V = V(P_n)\right) \wedge \left(E = E(P_n) \cup \{\{v_n, v_1\}\}\right) \wedge \left(C_n = (V, E)\right)$$

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

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

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

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

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

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

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

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

(1) TODO $\phi = \ldots$

$$Complement[\bar{G}, G] := \left(V = V(G)\right) \wedge \left(E = \{\{a, b\} \in V^{\{2\}} \mid (a \neq b) \wedge \left(\{a, b\} \notin E(G)\right)\}\right) \wedge \left(\bar{G} = (V, E)\right)$$

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

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

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

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

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

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

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

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

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

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

$KroneckerProperties := \ldots$

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

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

(1) TODO

$Tree[G] := (Connected[G]) \wedge \left(\nexists_{n,V_n}(Cycle[V_n, n, G])\right)$

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

(1) TODO

Chapter 2

Abstract Algebra

2.1 Functions

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

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

(1) TODO

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

(1) TODO

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

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

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

(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

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

(1) TODO

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

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

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

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

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

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

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

(1) TODO

2.3 Groups

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

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

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

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

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

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

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

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

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

  (3.1) TODO

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

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

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

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

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

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

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

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

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

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

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

2.4 Subgroups

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

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

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

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

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

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

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

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

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

(2.6) $Group[H,*]$

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

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

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

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

(1) TODO

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

(1) $Group[G,*]$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5 Special Groups

2.5.1 Cyclic Group

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5.2 Symmetric and Alternating Groups

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

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

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

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

2.5.3 Dihedral Group

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

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

2.6 Lagrange's Theorem

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(2) CyclicSubgroup of a non-identity element is G ▌ Non-identity elements generates G

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

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

2.7 Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) $Isomorphism[\phi, G, *, H, \diamond] \;\blacksquare\; (Homomorphism[\phi, G, *, H, \diamond]) \land (Bij[\phi, G, H])$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.8 Kernel and Image Homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.9 Conjugacy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(7) ==

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.10 Normal Subgroups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.11 Quotient Groups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3.1) $\phi(h_1) = h_1N = h_2N = \phi(h_2) \;\blacksquare\; \phi(h_1) = \phi(h_2)$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(9.2) $g \in G \;\blacksquare\; gK \in (G/K)$

(9.3) $\phi(gK) = gH = y \;\blacksquare\; y = \phi(gK)$

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

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

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

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

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