G.5. Proofs: Groups

Proposition G.5.1. — *Let G be a group and let H be a subgroup of G. Then the cosets of H in G partition G.*

Proof. —
To show: (a) If $g \in G$ then there exists $g' \in G$ such that $g \in g'H$.
(b) If $g_1H \cap g_2H \neq \emptyset$ then $g_1H = g_2H$.

(a) Let $g \in G$.
Since $1 \in H$ then $g = g \cdot 1 \in gH$.
So $g \in gH$.

(b) Assume $g_1H \cap g_2H \neq \emptyset$.
To show: (ba) $g_1H \subseteq g_2H$.
(bb) $g_2H \subseteq g_1H$.
Let $k \in g_1H \cap g_2H$.
Suppose $k = g_1h_1$ and $k = g_2h_2$, where $h_1, h_2 \in H$.
Then

$$g_1 = g_1h_1h_1^{-1} = kh_1^{-1} = g_2h_2h_1^{-1}, \quad \text{and}$$
$$g_2 = g_2h_2h_2^{-1} = kh_2^{-1} = g_1h_1h_2^{-1}.$$

(ba) Let $g \in g_1H$.
Then $g = g_1h$ for some $h \in H$.
Since $h_2h_1^{-1}h \in H$ then

$$g = g_1h = g_2h_2h_1^{-1}h \in g_2H.$$

So $g_1H \subseteq g_2H$.

(bb) Let $g \in g_2H$.
Then there exists $h \in H$ such that $g = g_2h$.
Since $h_1h_2^{-1}h \in H$ then

$$g = g_2h = g_1h_1h_2^{-1}h \in g_1H$$

So $g_2H \subseteq g_1H$.

So $g_1H = g_2H$.

So the cosets of H in G partition G. □

Proposition G.5.2. — *Let G be a group and let H be a subgroup of G. If g_1, $g_2 \in G$ then*

$$\mathrm{Card}(g_1H) = \mathrm{Card}(g_2H).$$

Proof. —
To show: There exists a bijection $\varphi\colon g_1H \to g_2H$.
Define

$$\begin{array}{rccc} \varphi\colon & g_1H & \to & g_2H \\ & x & \mapsto & g_2g_1^{-1}x. \end{array}$$

To show: (a) φ is well defined.
(b) φ is a bijection.

(a) To show: (aa) If $x \in g_1H$ then $\varphi(x) \in g_2H$.
(ab) If $x = y$ then $\varphi(x) = \varphi(y)$.

(aa) Assume $x \in g_1H$.

Then there exists $h \in H$ such that $x = g_1h$.
So $\varphi(x) = g_2g_1^{-1}g_1h = g_2h \in g_2H$.
(ab) Assume $x = y$.
Then $\varphi(x) = g_2g_1^1x = g_2g_1^{-1}y = \varphi(y)$.
So φ is well defined.

(b) Using that the inverse function exists if and only if φ is bijective, Theorem P.4.1,
To show: There exists an inverse map to φ.
Define

$$\begin{array}{rccc} \psi\colon & g_2H & \to & g_1H \\ & y & \mapsto & g_1g_2^{-1}y. \end{array}$$

HW: Show $\big($exactly as in (a) above$\big)$ that ψ is well defined.
Then

$$\psi(\varphi(x)) = g_1g_2^{-1}\varphi(x) = g_1g_2^{-1}g_2g_1^{-1}x = x, \quad \text{and}$$
$$\varphi(\psi(y)) = g_2g_1^{-1}\varphi(y) = g_2g_1^{-1}g_1g_2^{-1}y = y.$$

So ψ is an inverse function to φ.

So φ is a bijection. □

Corollary G.5.3. — *Let H be a subgroup of a group G. Then*

$$\mathrm{Card}(G) = \mathrm{Card}(G/H)\mathrm{Card}(H).$$

Proof. — By Proposition 1.1.4, all cosets in G/H are the same size as H.
Since the cosets of H partition G, the cosets are disjoint subsets of G,
and G is a union of these subsets.
So G is a union of $\mathrm{Card}(G/H)$ disjoint subsets all of which have size $\mathrm{Card}(H)$. □

Proposition G.5.4. — *Let N be a subgroup of G. The subgroup N is a normal subgroup of G if and only if G/N with the operation given by $(aN)(bN) = abN$ is a group.*

Proof. —
$\Longrightarrow$:
Assume N is a normal subgroup of G.
To show: (a) $(aN)(bN) = (abN)$ is a well defined operation on (G/N).
(b) N is the identity element of G/N.
(c) $g^{-1}N$ is the inverse of gN.

(a) To show: The function

$$\begin{array}{ccc} G/N \times G/N & \to & G/N \\ (aN, bN) & \mapsto & abN \end{array} \quad \text{is well defined.}$$

To show: If $(a_1N, b_1N), (a_2N, b_2N) \in G/N \times G/N$ and $(a_1N, b_1N) = (a_2N, b_2N)$ then $a_1b_1N = a_2b_2N$.
Assume $(a_1N, b_1N), (a_2N, b_2N) \in (G/N \times G/N)$ and $(a_1N, b_1N) = (a_2N, b_2N)$.
Then $a_1N = a_2N$ and $b_1N = b_2N$.
To show: (aa) $a_1b_1N \subseteq a_2b_2N$.
(ab) $a_2b_2N \subseteq a_1b_1N$.
(aa) Since $a_1N = a_2N$ then $a_1 = a_1 \cdot 1 \in a_2N$.
So there exists $n_1 \in N$ such that $a_1 = a_2n_1$.
Similary, there exists $n_2 \in N$ such that $b_1 = b_2n_2$ for some $n_2 \in N$.
Let $k \in a_1b_1N$.

Then $k = a_1b_1n$ for some $n \in N$. So

$$k = a_1b_1n = a_2n_1b_2n_2n = a_2b_2b_2^{-1}n_1b_2n_2n.$$

Since N is normal then $b_2^{-1}n_1b_2 \in N$, and therefore $(b_2^{-1}n_1b_2)n_2n \in N$.
So $k = a_2b_2(b_2^{-1}n_1b_2)n_2n \in a_2b_2N$.
So $a_1b_1N \subseteq a_2b_2N$.

(ab) Since $a_1N = a_2N$ then there exists $n_1 \in N$ such that $a_1n_1 = a_2$.
Since $b_1N = b_2N$ then there exists $n_2 \in N$ such that $b_1n_2 = b_2$.
Let $k \in a_2b_2N$.
Then there exists $n \in N$ such that $k = a_2b_2n$.
So

$$k = a_2b_2n = a_1n_1b_1n_2n = a_1b_1b_1^{-1}n_1b_1n_2n.$$

Since N is normal then $b_1^{-1}n_1b_1 \in N$, and therefore $(b_1^{-1}n_1b_1)n_2n \in N$.
So $k = a_1b_1(b_1^{-1}n_1b_1)n_2n \in a_1b_1N$.
So $a_2b_2N \subseteq a_1b_1N$.

So $(a_1b_1)N = (a_2b_2)N$.
So the operation is well defined.

(b) The coset $N = 1N$ is the identity since if $g \in G$ then

$$(N)(gN) = (1g)N = gN = (g1)N = (gN)(N),$$

(c) Given any coset gN, its inverse is $g^{-1}N$ since

$$(gN)(g^{-1}N) = (gg^{-1})N = N = g^{-1}gN = (g^{-1}N)(gN).$$

So G/N is a group.

$\Longleftarrow$:
Assume (G/N) is a group with operation $(aN)(bN) = abN$.
To show: If $g \in G$ and $n \in N$ then $gng^{-1} \in N$.

First we show: If $n \in N$ then $nN = N$.
Assume $n \in N$.
To show: (a) $nN \subseteq N$. (b) $N \subseteq nN$.

(a) Let $x \in nN$.
Then there exists $m \in N$ such that $x = nm$.
Since N is a subgroup then $nm \in N$.
So $x \in N$.
So $nN \subseteq N$.

(b) Assume $m \in N$.
Since N is a subgroup then $m = nn^{-1}m \in nN$.
So $N \subseteq nN$.

Now assume $g \in G$ and $n \in N$.
Then, by definition of the operation,

$$gng^{-1}N = (gN)(nN)(g^{-1}N) = (gN)(N)(g^{-1}N) = g1g^{-1}N = N.$$

So $gng^{-1} \in N$.
So N is a normal subgroup of G. □

Proposition G.5.5. — *Let $f\colon G \to H$ be a group homomorphism. Let 1_G and 1_H be the identities for G and H respectively. Then*
(a) $f(1_G) = 1_H$.
(b) For any $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

Proof. —
(a) Multiply both sides of the following equation by $f(1_G)^{-1}$:

$$f(1_G) = f(1_G \cdot 1_G) = f(1_G)f(1_G).$$

(b) Since $f(g)f(g^{-1}) = f(gg^{-1}) = f(1_G) = 1_H$ and $f(g^{-1})f(g) = f(g^{-1}g) = f(1_G) = 1_H$ then

$$f(g)^{-1} = f(g^{-1}).$$

□

Proposition G.5.6. — *Let $f\colon G \to H$ be a group homomorphism. Let 1_G and 1_H be the identities for G and H respectively. Then*
(a) $\ker f$ *is a normal subgroup of* G.
(b) $\mathrm{im} f$ *is a subgroup of* H.

Proof. —
To show: (a) $\ker f$ is a normal subgroup of G.
(b) $\mathrm{im} f$ is a subgroup of G.

(a) To show: (aa) $\ker f$ is a subgroup.
(ab) $\ker f$ is normal.

(aa) To show: (aaa) If $k_1, k_2 \in \ker f$ then $k_1k_2 \in \ker f$.
(aab) $1_G \in \ker f$.
(aac) If $k \in \ker f$ then $k^{-1} \in \ker f$.

(aaa) Assume $k_1, k_2 \in \ker f$.
Then $f(k_1) = 1_H$ and $f(k_2) = 1_H$.
So $f(k_1k_2) = f(k_1)f(k_2) = 1_H$.
So $k_1k_2 \in \ker f$.

(aab) Since $f(1_G) = 1_H$ then $1_G \in \ker f$.

(aac) Assume $k \in \ker f$.
Since $f(k) = 1_H$ then

$$f(k^{-1}) = f(k)^{-1} = 1_H^{-1} = 1_H.$$

So $k^{-1} \in \ker f$.

So $\ker f$ is a subgroup.

(ab) To show: If $g \in G$ and $k \in \ker f$ then $gkg^{-1} \in \ker f$.
Assume $g \in G$ and $k \in \ker f$.
Then

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(g^{-1}) = f(g)f(g)^{-1} = 1.$$

So $gkg^{-1} \in \ker f$.

So $\ker f$ is a normal subgroup of G.

(b) To show: $\mathrm{im} f$ is a subgroup of H.
To show: (ba) If $h_1, h_2 \in \mathrm{im} f$ then $h_1h_2 \in \mathrm{im} f$.
(bb) $1_H \in \mathrm{im} f$.
(bc) If $h \in \mathrm{im} f$ then $h^{-1} \in \mathrm{im} f$.

(ba) Assume $h_1, h_2 \in \mathrm{im} f$.
Then there exist $g_1, g_2 \in G$ such that $h_1 = f(g_1)$ and $h_2 = f(g_2)$.
Since f is a homomorphism then

$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2)$$

So $h_1h_2 \in \mathrm{im} f$.

(bb) By Proposition 1.1.11 (a), $f(1_G) = 1_H$.
So $1_H \in \mathrm{im} f$.
(bc) Assume $h \in \mathrm{im} f$.
Then there exists $g \in G$ such that $h = f(g)$.
Then, by Proposition 1.1.11 b),

$$h^{-1} = f(g)^{-1} = f(g^{-1}).$$

So $h^{-1} \in \mathrm{im} f$.
So $\mathrm{im} f$ is a subgroup of H.

□

Proposition G.5.7. — *Let $f: G \to H$ be a group homomorphism. Let 1_G be the identity in G. Then*
(a) $\ker f = (1_G)$ *if and only if f is injective.*
(b) $\mathrm{im} f = H$ *if and only if f is surjective.*

Proof. —
(a) Let 1_G and 1_H be the identities for G and H respectively.
$\Longrightarrow$: Assume $\ker f = (1_G)$.
To show: If $f(g_1) = f(g_2)$ then $g_1 = g_2$.
Assume $f(g_1) = f(g_2)$.
Then, by Proposition 1.1.11 b) and the fact that f is a homomorphism,

$$1_H = f(g_1)f(g_2)^{-1} = f(g_1 g_2^{-1}).$$

So $g_1 g_2^{-1} \in \ker f$.
But $\ker f = (1_G)$.
So $g_1 g_2^{-1} = 1_G$.
So $g_1 = g_2$.
So f is injective.
$\Longleftarrow$: Assume f is injective.
To show: (aa) $(1_G) \subseteq \ker f$.
(ab) $\ker f \subseteq (1_G)$.
(aa) Since $f(1_G) = 1_H$ then $1_G \in \ker f$.
So $(1_G) \subseteq \ker f$.
(ab) Let $k \in \ker f$.
Then $f(k) = 1_H$.
So $f(k) = f(1_G)$.
Thus, since f is injective then $k = 1_G$.
So $\ker f \subseteq (1_G)$.
So $\ker f = (1_G)$.
(b) $\Longrightarrow$: Assume $\mathrm{im} f = H$.
To show: If $h \in H$ then there exists $g \in G$ such that $f(g) = h$.
Assume $h \in H$.
Then $h \in \mathrm{im} f$.
So there exists some $g \in G$ such that $f(g) = h$.
So f is surjective.
$\Longleftarrow$: Assume f is surjective.
To show: (ba) $\mathrm{im} f \subseteq H$.
(bb) $H \subseteq \mathrm{im} f$.

(ba) Let $x \in \mathrm{im} f$.
Then $x = f(g)$ for some $g \in G$.
By the definition of f, $f(g) \in H$.
So $x \in H$.
So $\mathrm{im} f \subseteq H$.
(bb) Assume $x \in H$.
Since f is surjective there exists a g such that $f(g) = x$.
So $x \in \mathrm{im} f$.
So $H \subseteq \mathrm{im} f$.
So $\mathrm{im} f = H$. □

Theorem G.5.8. —
(a) *Let $f : G \to H$ be a group homomorphism and let $K = \ker f$. Define*

$$\begin{array}{cccc} \hat{f}: & G/\ker f & \longrightarrow & H \\ & gK & \longmapsto & f(g). \end{array}$$

Then $\hat{f}$ is a well defined injective group homomorphism.
(b) *Let $f : G \to H$ be a group homomorphism and define*

$$\begin{array}{cccc} f': & G & \longrightarrow & \mathrm{im} f \\ & g & \mapsto & f(g). \end{array}$$

Then f' is a well defined surjective group homomorphism.
(c) *If $f : G \to H$ is a group homomorphism then*

$$G/\ker f \simeq \mathrm{im} f,$$

where the isomorphism is a group isomorphism.

Proof. —
(a) To show: (aa) $\hat{f}$ is well defined.
(ab) $\hat{f}$ is injective.
(ac) $\hat{f}$ is a homomorphism.
(aa) To show: (aaa) If $g \in G$ then $\hat{f}(gK) \in H$.
(aab) If $g_1K = g_2K$ then $\hat{f}(g_1K) = \hat{f}(g_2K)$.
(aaa) Assume $g \in G$.
Then $\hat{f}(gK) = f(g)$ and $f(g) \in H$, by the definition of $\hat{f}$ and f.
(aab) Assume $g_1K = g_2K$.
Then there exists $k \in K$ such that $g_1 = g_2k$.
To show: $\hat{f}(g_1K) = \hat{f}(g_2K)$.
To show: $f(g_1) = f(g_2)$.
Since $k \in \ker f$ then $f(k) = 1$ and so

$$f(g_1) = f(g_2k) = f(g_2)f(k) = f(g_2).$$

So $\hat{f}(g_1K) = \hat{f}(g_2K)$.
So $\hat{f}$ is well defined.
(ab) To show: If $\hat{f}(g_1K) = \hat{f}(g_2K)$ then $g_1K = g_2K$.
Assume $\hat{f}(g_1K) = \hat{f}(g_2K)$.
Then $f(g_1) = f(g_2)$.
So $f(g_2)^{-1}f(g_1) = 1$.
So $f(g_2^{-1}g_1) = 1$.

So $g_2^{-1}g_1 \in \ker f$.
So there exists $k \in \ker f$ such that $g_2^{-1}g_1 = k$.
So there exists $k \in \ker f$ such that $g_1 = g_2k$.
To show: (aba) $g_1K \subseteq g_2K$.
(abb) $g_2K \subseteq g_1K$.

(aba) Let $g \in g_1K$.
Then there exists $k_1 \in K$ such that $g = g_1k_1$.
So $g = g_2kk_1 \in g_2K$, since $kk_1 \in K$.
So $g_1K \subseteq g_2K$.

(abb) Let $g \in g_2K$.
Then there exists $k_2 \in K$ such that $g = g_2k_2$.
So $g = g_1k^{-1}k_2 \in g_1K$ since $k^{-1}k_2 \in K$.
So $g_2K \subseteq g_1K$.

So $g_1K = g_2K$.
So $\hat{f}$ is injective.

(ac) To show: $\hat{f}(g_1K)\hat{f}(g_2K) = \hat{f}\big((g_1K)(g_2K)\big)$.
Since f is a homomorphism,

$$\hat{f}(g_1K)\hat{f}(g_2K) = f(g_1)f(g_2) = f(g_1g_2) = \hat{f}(g_1g_2K) = \hat{f}\big((g_1K)(g_2K)\big).$$

So $\hat{f}$ is a homomorphism.

(b) To show: (ba) f' is well defined.
(bb) f' is surjective.
(bc) f' is a homomorphism.

(ba) and (bb) are proved in Ex. 2.2.3, Part I.
(bc) Since f is a homomorphism,

$$f'(g)f'(h) = f(g)f(h) = f(gh) = f'(gh).$$

(c) Let $K = \ker f$.
By a), the function

$$\begin{array}{rccc} \hat{f}\colon & G/K & \longrightarrow & H \\ & gK & \longmapsto & f(g) \end{array}$$

is a well defined injective homomorphism.
By b), the function

$$\begin{array}{rccc} \hat{f}'\colon & G/K & \longrightarrow & \mathrm{im}\hat{f} \\ & gK & \longmapsto & \hat{f}(gK) = f(g) \end{array}$$

is a well defined surjective homomorphism.
To show: (ca) $\mathrm{im}\hat{f} = \mathrm{im}f$.
(cb) $\hat{f}'$ is injective.

(ca) To show: (caa) $\mathrm{im}\hat{f} \subseteq \mathrm{im}f$.
(cab) $\mathrm{im}f \subseteq \mathrm{im}\hat{f}$.

(caa) Let $h \in \mathrm{im}\hat{f}$.
Then there exists $gK \in G/K$ such that $\hat{f}(gK) = h$.
Let $g' \in gK$.
Then there exists $k \in K$ such that $g' = gk$.
Since f is a homomorphism and $f(k) = 1$ then

$$f(g') = f(gk) = f(g)f(k) = f(g) = \hat{f}(gK) = h.$$

So $h \in \mathrm{im} f$.
So $\mathrm{im}\hat{f} \subseteq \mathrm{im} f$.
(cab) Let $h \in \mathrm{im} f$.
Then there exists $g \in G$ such that $f(g) = h$.
So $\hat{f}(gK) = f(g) = h$.
So $h \in \mathrm{im}\hat{f}$.
So $\mathrm{im} f \subseteq \mathrm{im}\hat{f}$.

(cb) To show: If $\hat{f}'(g_1K) = \hat{f}'(g_2K)$ then $g_1K = g_2K$.
Assume $\hat{f}'(g_1K) = \hat{f}'(g_2K)$.
Then $\hat{f}(g_1K) = \hat{f}(g_2K)$.
Then, since $\hat{f}$ is injective, $g_1K = g_2K$.

So $\hat{f}'$ is injective.
Thus

$$\begin{array}{rccc} \hat{f}': & G/K & \longrightarrow & \mathrm{im}\hat{f} \\ & gK & \longmapsto & f(g) \end{array}$$

is a well defined bijective homomorphism. $\square$