§1P. Groups

(1.1.3) Proposition. *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 $g \in g'H$ for some $g' \in G$.
b) If $g_1H \cap g_2H \neq \emptyset$ then $g_1H = g_2H$.

a) Let $g \in G$.
Then $g = g \cdot 1 \in gH$ since $1 \in H$.
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 $h \in H$.
Then

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

since $h_2h_1^{-1}h \in H$.
So $g_1H \subseteq g_2H$.
bb) Let $g \in g_2H$.
Then $g = g_2h$ for some $h \in H$.
So

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

since $h_1h_2^{-1}h \in H$.
So $g_2H \subseteq g_1H$.
So $g_1H = g_2H$.
So the cosets of H in G partition G. □

(1.1.4) Proposition. *Let G be a group and let H be a subgroup of G. Then for any g_1, $g_2 \in G$,*

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

Proof.

To show: There is a bijection from g_1H to g_2H.
Define a map φ by

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

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 $x = g_1h$ for some $h \in H$.
So $\varphi(x) = g_2g_1^{-1}g_1h = g_2h \in g_2H$.

ab) This is clear from the definition of φ.

So φ is well defined.

b) By virtue of Theorem 2.2.3, Part I, we want to construct an inverse map for φ. Define

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

HW: Show (exactly as in a) above) 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. □

(1.1.5) Corollary. *Let H be a subgroup of a group G. Then*

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

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 $\text{Card}(G/H)$ disjoint subsets all of which have size $\text{Card}(H)$. □

(1.1.8) Proposition. *Let N be a subgroup of G. 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) We want the operation on G/N given by

$$\begin{array}{ccc} G/N \times G/N & \to & G/N \\ (aN, bN) & \mapsto & abN \end{array}$$

to be 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 $a_1b_1N = a_2b_2N$.
Let $(a_1N, b_1N), (a_2N, b_2N) \in (G/N \times G/N)$ such that $(a_1N, b_1N) = (a_2N, b_2N)$.
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) We know $a_1 = a_1 \cdot 1 \in a_2N$ since $a_1N = a_2N$.

So $a_1 = a_2 n_1$ for some $n_1 \in N$.
Similary, $b_1 = b_2 n_2$ for some $n_2 \in N$.
Let $k \in a_1 b_1 N$.
Then $k = a_1 b_1 n$ for some $n \in N$. So

$$\begin{aligned} k &= a_1 b_1 n \\ &= a_2 n_1 b_2 n_2 n \\ &= a_2 b_2 b_2^{-1} n_1 b_2 n_2 n. \end{aligned}$$

Since N is normal, $b_2^{-1} n_1 b_2 \in N$, and therefore $(b_2^{-1} n_1 b_2) n_2 n \in N$.
So $k = a_2 b_2 (b_2^{-1} n_1 b_2) n_2 n \in a_2 b_2 N$.
So $a_1 b_1 N \subseteq a_2 b_2 N$.

ab) Since $a_1 N = a_2 N$, we know $a_1 n_1 = a_2$ for some $n_1 \in N$.
Since $b_1 N = b_2 N$, we know $b_1 n_2 = b_2$ for some $n_2 \in N$.
Let $k \in a_2 b_2 N$.
Then $k = a_2 b_2 n$ for some $n \in N$. So

$$\begin{aligned} k &= a_2 b_2 n \\ &= a_1 n_1 b_1 n_2 n \\ &= a_1 b_1 b_1^{-1} n_1 b_1 n_2 n. \end{aligned}$$

Since N is normal $b_1^{-1} n_1 b_1 \in N$, and therefore $(b_1^{-1} n_1 b_1) n_2 n \in N$.
So $k = a_1 b_1 (b_1^{-1} n_1 b_1) n_2 n \in a_1 b_1 N$.
So $a_2 b_2 N \subseteq a_1 b_1 N$.

So $(a_1 b_1) N = (a_2 b_2) N$.
So the operation is well defined.

b) The coset $N = 1N$ is the identity since

$$\begin{aligned} (N)(gN) &= (1g)N \\ &= gN \\ &= (g1)N \\ &= (gN)(N), \end{aligned}$$

for all $g \in G$.

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

$$\begin{aligned} (gN)(g^{-1}N) &= (gg^{-1})N \\ &= N \\ &= g^{-1}gN \\ &= (g^{-1}N)(gN). \end{aligned}$$

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 $x = nm$ for some $m \in N$.
Since N is a subgroup, $nm \in N$.
So $x \in N$.
So $nN \subseteq N$.

b) Assume $m \in N$.
Then, since N is a subgroup, $m = nn^{-1}m \in nN$.
So $N \subseteq nN$.

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

$$\begin{aligned} gng^{-1}N &= (gN)(nN)(g^{-1}N) \\ &= (gN)(N)(g^{-1}N) \\ &= g1g^{-1}N \\ &= N. \end{aligned}$$

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

(1.1.11) Proposition. *Let $f: G \to H$ 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

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

(1.1.13) Proposition. *Let $f: G \to H$ 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) $\operatorname{im} f$ is a subgroup of H.

Proof.

To show: a) $\ker f$ is a normal subgroup of G.
b) $\operatorname{im} f$ 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 $f(1_G) = 1_H$, $1_G \in \ker f$.
aac) Assume $k \in \ker f$. So $f(k) = 1_H$.
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

$$\begin{aligned} f(gkg^{-1}) &= f(g)f(k)f(g^{-1}) \\ &= f(g)f(g^{-1}) \\ &= f(g)f(g)^{-1} \\ &= 1. \end{aligned}$$

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

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

b) To show: $\operatorname{im} f$ is a subgroup of H.

To show: ba) If $h_1, h_2 \in \operatorname{im} f$ then $h_1h_2 \in \operatorname{im} f$.

bb) $1_H \in \operatorname{im} f$.

bc) If $h \in \operatorname{im} f$ then $h^{-1} \in \operatorname{im} f$.

ba) Assume $h_1, h_2 \in \operatorname{im} f$.

Then $h_1 = f(g_1)$ and $h_2 = f(g_2)$ for some $g_1, g_2 \in G$.

Then

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

since f is a homomorphism.

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

bb) By Proposition 1.1.11 a), $f(1_G) = 1_H$, so $1_H \in \operatorname{im} f$.

bc) Assume $h \in \operatorname{im} f$.

Then $h = f(g)$ for some $g \in G$.

Then, by Proposition 1.1.11 b),

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

So $h^{-1} \in \operatorname{im} f$.

So $\operatorname{im} f$ is a subgroup of H. □

(1.1.14) Proposition. *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) $\operatorname{im} f = H$ *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,

$$1_H = f(g_1)f(g_2)^{-1} = f(g_1g_2^{-1}).$$

So $g_1g_2^{-1} \in \ker f$.

But $\ker f = (1_G)$.

So $g_1g_2^{-1} = 1_G$.

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 $f(1_G) = 1_H$, $1_G \in \ker f$.
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, $k = 1_G$.
So $\ker f \subseteq (1_G)$.

So $\ker f = (1_G)$.

b) $\Longrightarrow$: Assume $\operatorname{im} f = H$.
To show: If $h \in H$ then there exists $g \in G$ such that $f(g) = h$.
Assume $h \in H$.
Then $h \in \operatorname{im} f$.
So there exists some $g \in G$ such that $f(g) = h$.
So f is surjective.

$\Longleftarrow$: Assume f is surjective.
To show: ba) $\operatorname{im} f \subseteq H$.
bb) $H \subseteq \operatorname{im} f$.

ba) Let $x \in \operatorname{im} f$.
Then $x = f(g)$ for some $g \in G$.
By the definition of f, $f(g) \in H$.
So $x \in H$.
So $\operatorname{im} f \subseteq H$.

bb) Assume $x \in H$.
Since f is surjective there exists a g such that $f(g) = x$.
So $x \in \operatorname{im} f$.
So $H \subseteq \operatorname{im} f$.

So $\operatorname{im} f = H$. □

(1.1.15) Theorem.

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

$$\begin{array}{rccc} \hat{f}: & G/\ker f & \to & H \\ & gK & \mapsto & f(g). \end{array}$$

Then $\hat{f}$ is a well defined injective group homomorphism.

b) Let $f: G \to H$ be a group homomorphism and define

$$\begin{array}{rccc} f': & G & \to & \operatorname{im} f \\ & g & \mapsto & f(g). \end{array}$$

Then f' is a well defined surjective group homomorphism.

c) If $f: G \to H$ is a group homomorphism then

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

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 $g_1 = g_2k$ for some $k \in K$.
To show: $\hat{f}(g_1K) = \hat{f}(g_2K)$, i.e.,
To show: $f(g_1) = f(g_2)$.
Since $k \in \ker f$, we have $f(k) = 1$ 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 $f(g_1)f(g_2)^{-1} = 1$.
So $f(g_1g_2^{-1}) = 1$.
So $g_1g_2^{-1} \in \ker f$.
So $g_1g_2^{-1} = k$ for some $k \in \ker f$.
So $g_1 = g_2k$ for some $k \in \ker f$.
To show: aba) $g_1K \subseteq g_2K$.
abb) $g_2K \subseteq g_1K$.

aba) Let $g \in g_1K$. Then $g = g_1k_1$ for some $k_1 \in K$.
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 $g = g_2k_2$ for some $k_2 \in K$.
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,

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

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,

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

So f' is a homomorphism.

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

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

is a well defined injective homomorphism.

By b), the function

$$\begin{array}{rccc} \hat{f}'\colon & G/K & \to & \operatorname{im} \hat{f} \\ & gK & \mapsto & \hat{f}(gK) = f(g) \end{array}$$

is a well defined surjective homomorphism.

To show: ca) $\operatorname{im} \hat{f} = \operatorname{im} f$.
cb) $\hat{f}'$ is injective.

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

caa) Let $h \in \operatorname{im} \hat{f}$.
Then there is some $gK \in G/K$ such that $\hat{f}(gK) = h$.
Let $g' \in gK$.
Then $g' = gk$ for some $k \in K$.
Then, since f is a homomorphism and $f(k) = 1$,

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

So $h \in \operatorname{im} f$.
So $\operatorname{im} \hat{f} \subseteq \operatorname{im} f$.

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

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 we have

$$\begin{array}{rccc} \hat{f}'\colon & G/K & \to & \operatorname{im} \hat{f} \\ & gK & \mapsto & f(g) \end{array}$$

is a well defined bijective homomorphism. □

(1.2.3) Proposition. *Suppose G is a group acting on a set S and let $s \in S$ and $g \in G$. Then*
a) G_s is a subgroup of G.
b) $G_{gs} = gG_sg^{-1}$.

Proof.

a)To show: aa) If $h_1, h_2 \in G_s$ then $h_1h_2 \in G_s$
ab) $1 \in G_s$.
ac) If $h \in G_s$ then $h^{-1} \in G_s$.

aa) Assume $h_1, h_2 \in G_s$. Then

$$(h_1h_2)s = h_1(h_2s) = h_1s = s.$$

So $h_1h_2 \in G_s$.

ab) Since $1s = s, 1 \in G_s$.

ac) Assume $h \in G_s$. Then

$$h^{-1}s = h^{-1}(hs) = (h^{-1}h)s = 1s = s.$$

So $h^{-1} \in G_s$.

So G_s is a subgroup of G.

b) To show: ba) $G_{gs} \subseteq gG_sg^{-1}$.
bb) $gG_sg^{-1} \subseteq G_{gs}$.

ba) Assume $h \in G_{gs}$.
Then $hgs = gs$.
So $g^{-1}hgs = s$.
So $g^{-1}hg \in G_s$.
Since $h = g(g^{-1}hg)g^{-1},\ h \in gG_sg^{-1}$.
So $G_{gs} \subseteq gG_sg^{-1}$.

bb) Assume $h \in gG_sg^{-1}$.
So $h = gag^{-1}$ for some $a \in G_s$.
Then

$$hgs = (gag^{-1})gs = gas = gs.$$

So $h \in G_{gs}$.
So $G_{gs} \subseteq gG_sg^{-1}$.

So $G_{gs} = gG_sg^{-1}$. □

(1.2.4) Proposition. *Let G be a group which acts on a set S. Then the orbits partition the set S.*

Proof.

To show: a) If $s \in S$ then $s \in Gt$ for some $t \in S$.
b) If $s_1, s_2 \in S$ and $Gs_1 \cap Gs_2 \neq \emptyset$ then $Gs_1 = Gs_2$.

a) Assume $s \in S$.
Then, since $s = 1s, s \in Gs$.

b) Assume $s_1, s_2 \in S$ and that $Gs_1 \cap Gs_2 \neq \emptyset$.
Then let $t \in Gs_1 \cap Gs_2$.
So $t = g_1s_1$ and $t = g_2s_2$ for some elements $g_1, g_2 \in G$.
So

$$s_1 = g_1^{-1}g_2s_2 \text{ and } s_2 = g_2^{-1}g_1s_1.$$

To show: $Gs_1 = Gs_2$.
To show: ba) $Gs_1 \subseteq Gs_2$.

bb) $Gs_2 \subseteq Gs_1$.

ba) Let $t_1 \in Gs_1$.
So $t = h_1 s_1$ for some $h_1 \in G$.
Then

$$t_1 = h_1 s_1 = h_1 g_1^{-1} g_2 s_2 \in Gs_2.$$

So $Gs_1 \subseteq Gs_2$.

bb) Let $t_2 \in Gs_s$.
So $t_2 = h_2 s_2$ for some $h_2 \in G$.
Then

$$t_2 = h_2 s_2 = h_2 g_2^{-1} g_1 s_1 \in Gs_1.$$

So $Gs_2 \subseteq Gs_1$.

So $Gs_1 = Gs_2$.

So the orbits partition S. □

(1.2.5) Corollary. *If G is a group acting on a set S and Gs_i denote the orbits of the action of G on S then*

$$\text{Card}(S) = \sum_{\substack{\text{distinct} \\ \text{orbits}}} \text{Card}(Gs_i).$$

Proof.
By Proposition 1.2.4, S is a disjoint union of orbits.
So Card(S) is the sum of the cardinalities of the orbits. □

(1.2.6) Proposition. *Let G be a group acting on a set S and let $s \in S$. If Gs is the orbit containing s and G_s is the stabilizer of s then*

$$| G{:}G_s | = \text{Card}(Gs).$$

where $| G{:}G_s |$ is the index of $G_s \in G$.

Proof.
Recall that $| G{:}G_s | = \text{Card}(G/G_s)$.
To show: There is a bijective map

$$\varphi\colon \ G/G_s \to Gs.$$

Let us define

$$\begin{array}{rccc} \varphi\colon & G/G_s & \to & Gs \\ & gG_s & \mapsto & gs. \end{array}$$

To show: a) φ is well defined.
b) φ is bijective.

a) To show: aa) $\varphi(gG_s) \in Gs$ for every $g \in G$.
ab) If $g_1 G_s = g_2 G_s$ then $\varphi(g_1 G_s) = \varphi(g_2 G_s)$.

aa) Is clear from the definition of φ, $\varphi(gG_s) = gs \in Gs$.

ab) Assume $g_1, g_2 \in G$ and $g_1 G_s = g_2 G_s$.
Then $g_1 = g_2 h$ for some $h \in G_s$.
To show: $g_1 s = g_2 s$.
Then

$$g_1 s = g_2 hs = g_2 s,$$

since $h \in G_s$.
So $\varphi(g_1G_s) = \varphi(g_2G_s)$.
So φ is well defined.

b) To show: ba) φ is injective, i.e. if $\varphi(g_1G_s) = \varphi(g_2G_2)$ then $g_1G_s = g_2G_s$.
bb) φ is surjective, i.e. if $gs \in G_s$ then there exists $hG_s \in G/G_s$ such that $\varphi(hG_s) = gs$.

ba) Assume $\varphi(g_1G_s) = \varphi(g_2G_s)$.
Then $g_1s = g_2s$.
So $s = g_1^{-1}g_2s$ and $g_2^{-1}g_1s = s$.
So $g_1^{-1}g_2 \in G_s$ and $g_2^{-1}g_1 \in G_s$.
To show: φ is injective.
To show: $g_1G_s = g_2G_s$
To show: baa) $g_1G_s \subseteq g_2G_s$.
bab) $g_2G_s \subseteq g_1G_s$.

baa) Let $k_1 \in g_1G_s$.
So $k_1 = g_1h_1$ for some $h_1 \in G_s$.
Then

$$k_1 = g_1h_1 = g_1g_1^{-1}g_2g_2^{-1}g_1h_1 = g_2(g_2^{-1}g_1h_1) \in g_2G_s.$$

So $g_1G_s \subseteq g_2G_s$.

bab) Let $k_2 \in g_2G_s$.
So $k_2 = g_2h_2$ for some $h_2 \in G_s$.
Then

$$k_2 = g_2h_2 = g_2g_2^{-1}g_1g_1^{-1}g_2h_2 = g_1(g_1^{-1}g_2h_2) \in g_1G_s.$$

So $g_2G_s \subseteq g_1G_s$.
So $g_1G_s = g_2G_s$.
So φ is injective.

bb) To show: φ is surjective.
Assume $t \in G_s$.
Then $t = gs$ for some $g \in G$.
Thus,

$$\varphi(gG_s) = gs = t.$$

So φ is surjective.
So φ is bijective. □

(1.2.7) Corollary. *Let G be a group acting on a set S. Let $s \in S$, let G_s denote the stabilizer of s, and let Gs denote the orbit of s. Then*

$$\mathrm{Card}(G) = \mathrm{Card}(Gs)\mathrm{Card}(G_s).$$

Proof.
Multiply both sides of the identity in Proposition 1.2.6 by $\mathrm{Card}(G_s)$ and use Corollary 1.1.5. □

(1.2.9) Proposition. *Let H be a subgroup of G and let N_H be the normalizer of H in G. Then*
a) H is a normal subgroup of N_H.
b) If K is a subgroup of G such that $H \subseteq K \subseteq G$ and H is a normal subgroup of K then $K \subseteq N_H$.

Proof.

b) Let $k \in K$.
To show: $k \in N_H$.
To show: $khk^{-1} \in H$ for all $h \in H$.
This is true since H is normal in K.
So $K \subseteq N_H$.

a) This is the special case of b) when $K = H$. □

(1.2.10) Proposition. *Let G be a group and let $\mathcal{S}$ be the set of subsets of G. Then*

a) G acts on $\mathcal{S}$ by

$$\begin{array}{rccc} \alpha: & G \times \mathcal{S} & \to & \mathcal{S} \\ & (g, S) & \mapsto & gSg^{-1} \end{array}$$

where $gSg^{-1} = \{gsg^{-1} \mid s \in S\}$. We say that G acts on $\mathcal{S}$ by conjugation.

b) If S is a subset of G then N_S is the stabilizer of S under the action of G on $\mathcal{S}$ by conjugation.

Proof.

a) To show: aa) α is well defined.
ab) $\alpha(1, S) = S$ for all $S \in \mathcal{S}$.
ac) $\alpha(g, \alpha(h, S)) = \alpha(gh, S)$ for all $g, h \in G$, and $S \in \mathcal{S}$.

aa) To show: aaa) $gSg^{-1} \in \mathcal{S}$.
aab) If $S = T$ and $g = h$ then $gSg^{-1} = hTh^{-1}$.
Both of these are clear from the definitions.

ab) Let $S \in \mathcal{S}$.
Then

$$\alpha(1, S) = 1S1^{-1} = S.$$

ac) Let $g, h \in G$ and $S \in \mathcal{S}$.
Then

$$\begin{aligned} \alpha\big(g, \alpha(h, S)\big) &= \alpha(g, hSh^{-1}) = g(hSh^{-1})g^{-1} \\ &= (gh)S(h^{-1}g^{-1}) = (gh)S(gh)^{-1} = \alpha(gh, S). \end{aligned}$$

b) This follows immediately from the definitions of N_S and of stabilizer. □

(1.2.12) Proposition. *Let G be a group. Then*

a) G acts on G by

$$\begin{array}{ccc} G \times G & \to & G \\ (g, s) & \mapsto & gsg^{-1}. \end{array}$$

We say that G acts on itself by conjugation.

b) Two elements $g_1, g_2 \in G$ are conjugate if and only if they are in the same orbit under the action of G on itself by conjugation.

c) The conjugacy class, $\mathcal{C}_g$, of $g \in G$ is the orbit of g under the action of G on itself by conjugation.

d) The centralizer, Z_g, of $g \in G$ is the stablilizer of g under the action of G on itself by conjugation.

Proof.

a) The proof is exactly the same as the proof of a) in Proposition 1.2.10.
Replace all the capital S's by lower case s's.

b), c), and d) follow easily from the definitons. □

(1.2.14) Lemma. *Let G_s be the stabilizer of $s \in G$ under the action of G on itself by conjugation. Then*

a) For each subset $S \subseteq G$,

$$Z_S = \bigcap_{s \in S} G_s.$$

b) $Z(G) = Z_G$, *where* $Z(G)$ *denotes the center of* G.
c) $s \in Z(G)$ *if and only if* $Z_S = G$.
d) $s \in Z(G)$ *if and only if* $\mathcal{C}_s = \{s\}$.

Proof.

a) aa) Assume $s \in Z_s$.
Then $sxs^{-1} = s$ for all $s \in S$.
So $x \in G_s$ for all $s \in S$.
So $x \cap_{s \in S} G_s$.
So $Z_s \subseteq \cap_{s \in S} G_s$.
ab) Assume $x \in \cap_{s \in S} G_s$.
Then $xsx^{-1} = s$ for all $s \in S$.
So $x \in Z_s$.
So $\cap_{s \in S} G_s$.

b) This is clear from the definitions of Z_G and $Z(G)$.

c) $\Longrightarrow$: Let $s \in Z(G)$.
To show: $Z_S = G$.
By definiton $Z_S \subseteq G$.
To show: $G \subseteq Z_S$.
Let $g \in G$.
Then $gsg^{-1} = s$ since $s \in Z(G)$.
So $g \in Z_S$.
So $G \subseteq Z_S$.
So $Z_S = G$.

$\Longleftarrow$: Assume $Z_S = G$.
Then $gsg^{-1} = s$ for all $g \in G$.
So $gs = sg$ for all $g \in G$.
So $s \in Z(G)$.

d) $\Longrightarrow$: Assume $s \in Z(G)$.
Then $gsg^{-1} = s$ for all $s \in G$.
So $\mathcal{C}_s = \{gsg^{-1} \mid g \in G\} = \{s\}$.

$\Longleftarrow$: Assume $\mathcal{C}_s = \{s\}$.
Then $gsg^{-1} = s$ for all $g \in G$.
So $s \in Z(g)$. □

(1.2.15) Proposition. *(The Class Equation) Let* $\mathcal{C}_{g_i}$ *denote the conjugacy classes in a group* G *and let* $|\mathcal{C}_{g_i}|$ *denote* $\text{Card}(\mathcal{C}_{g_i})$. *Then*

$$|G| = |Z(G)| + \sum_{|\mathcal{C}_{g_i}|>1} \text{Card}(\mathcal{C}_{g_i}).$$

Proof.

By Corollary 1.2.5 and the fact that the $\mathcal{C}_{g_i}$ are the orbits of G acting on itself by conjugation we know that

$$|G| = \sum_{\mathcal{C}_{g_i}} \text{Card}(\mathcal{C}_{g_i}).$$

By Lemma 1.2.14 d) we know that

$$Z(G) = \bigcup_{|\mathcal{C}_{g_i}|=1} \mathcal{C}_{g_i}.$$

So

$$\begin{aligned} |G| &= \sum_{|\mathcal{C}_{g_i}|=1} \mathrm{Card}(\mathcal{C}_{g_i}) + \sum_{|\mathcal{C}_{g_i}|>1} \mathrm{Card}(\mathcal{C}_{g_i}) \\ &= \mathrm{Card}\big(Z(G)\big) + \sum_{|\mathcal{C}_{g_i}|>1} \mathrm{Card}(\mathcal{C}_{g_i}). \quad \square \end{aligned}$$