Chapter 2. SETS AND FUNCTIONS

§1P. Sets

1. *DeMorgan's Laws.* Let A, B, and C be sets. Show that

a) $(A \cup B) \cup C = A \cup (B \cup C)$.
b) $A \cup B = B \cup A$.
c) $A \cup \emptyset = A$.
d) $(A \cap B) \cap C = A \cap (B \cap C)$.
e) $A \cap B = B \cap A$.
f) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof.

a) To show: aa) $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.
ab) $A \cup (B \cup C) \subseteq (A \cup B) \cup C$.

aa) Let $x \in (A \cup B) \cup C$.
Then $x \in A \cup B$ or $x \in C$.
So $x \in A$ or $x \in B$ or $x \in C$.
So $x \in A$ or $x \in B \cup C$.
So $x \in A \cup (B \cup C)$.
So $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.

ab) Let $x \in A \cup (B \cup C)$.
Then $x \in A$ or $x \in B \cup C$.
So $x \in A$ or $x \in B$ or $x \in C$.
So $x \in A \cup B$ or $x \in C$.
So $x \in (A \cup B) \cup C$.
So $A \cup (B \cup C) \subseteq (A \cup B) \cup C$.

So $(A \cup B) \cup C = A \cup (B \cup C)$.

b) To show: ba) $A \cup B \subseteq B \cup A$.
bb) $B \cup A \subseteq A \cup B$.

ba) Let $x \in A \cup B$.
Then $x \in A$ or $x \in B$.
So $x \in B$ or $x \in A$.
So $x \in B \cup A$.
So $A \cup B \subseteq B \cup A$.

bb) Let $x \in B \cup A$.
Then $x \in B$ or $x \in A$.
So $x \in A$ or $x \in B$.
So $x \in A \cup B$.
So $B \cup A \subseteq A \cup B$.

So $A \cup B = B \cup A$.

c) To show: ca) $A \cup \emptyset \subseteq A$.
cb) $A \subseteq A \cup \emptyset$.

ca) Proof by contradiction.
Assume $A \cup \emptyset \not\subseteq A$.
Then there exists $x \in A \cup \emptyset$ such that $x \notin A$.
So $x \in \emptyset$.
This is a contradiction to the definition of empty set.
So $A \cup \emptyset \subseteq A$.

cb) Let $x \in A$.
Then $x \in A$ or $x \in \emptyset$.

So $x \in A \cup \emptyset$.
So $A \subseteq A \cup \emptyset$.

So $A \cup \emptyset = A$.

d) To show: da) $(A \cap B) \cap C \subseteq A \cap (B \cap C)$.
db) $A \cap (B \cap C) \subseteq (A \cap B) \cap C$.

da) Let $x \in (A \cap B) \cap C$.
Then $x \in A \cap B$ and $x \in C$.
So $x \in A$ and $x \in B$ and $x \in C$.
So $x \in A$ and $x \in B \cap C$.
So $x \in A \cap (B \cap C)$.
So $(A \cap B) \cap C \subseteq A \cap (B \cap C)$.

db) Let $x \in A \cap (B \cap C)$.
Then $x \in A$ and $x \in B \cap C$.
So $x \in A$ and $x \in B$ and $x \in C$.
So $x \in A \cap B$ and $x \in C$.
So $x \in (A \cap B) \cap C$.
So $A \cap (B \cap C) \subseteq (A \cap B) \cap C$.

So $(A \cap B) \cap C = A \cap (B \cap C)$.

e) To show: ea) $A \cap B \subseteq B \cap A$.
eb) $B \cap A \subseteq A \cap B$.

ea) Let $x \in A \cap B$.
Then $x \in A$ and $x \in B$.
So $x \in B$ and $x \in A$.
So $x \in B \cap A$.
So $A \cap B \subseteq B \cap A$.

eb) Let $x \in B \cap A$.
Then $x \in B$ and $x \in A$.
So $x \in A$ and $x \in B$.
So $x \in A \cap B$.
So $B \cap A \subseteq A \cap B$.

So $A \cap B = B \cap A$.

f) To show: fa) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
fb) $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

fa) Let $x \in A \cap (B \cup C)$.
Then $x \in A$ and $x \in B \cup C$.
So $x \in A$ and $x \in B$ or $x \in C$.
So $x \in A$ and $x \in B$, or $x \in A$ and $x \in C$.
So $x \in A \cap B$ or $x \in A \cap C$.
So $x \in (A \cap B) \cup (A \cap C)$.
So $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

fb) Let $x \in (A \cap B) \cup (A \cap C)$.
Then $x \in A \cap B$ or $x \in A \cap C$.
So $x \in A$ and $x \in B$, or $x \in A$ and $x \in C$.
So $x \in A$ and, $x \in B$ or $x \in C$.
So $x \in A$ and $x \in B \cup C$.
So $x \in A \cap (B \cup C)$.
So $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

So $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. $\square$

§2P. Functions

(2.2.3) Proposition. *Let $f: S \to T$ be a function. An inverse function to f exists if and only if f is bijective.*

Proof.

$\Longrightarrow$: Assume $f: S \to T$ has an inverse function $f^{-1}: T \to S$.
To show: a) f is injective.
b) f is surjective.

a) Assume $f(s_1) = f(s_2)$.
To show: $s_1 = s_2$.

$$s_1 = f^{-1}\big(f(s_1)\big) = f^{-1}\big(f(s_2)\big) = s_2.$$

So f is injective.

b) Let $t \in T$.
To show: There exists $s \in S$ such that $f(s) = t$.
Let $s = f^{-1}(t)$.
Then

$$f(s) = f\big(f^{-1}(t)\big) = t.$$

So f is surjective.

So f is bijective.

$\Longleftarrow$: Assume $f: S \to T$ is bijective.
To show: f has an inverse function.
We need to define a function $\varphi: T \to S$.
Let $t \in T$.
Since f is surjective there exists $s \in S$ such that $f(s) = t$.
Define $\varphi(t) = s$.
To show: a) φ is well defined.
b) φ is an inverse function to f.

a) To show: aa) If $t \in T$ then $\varphi(t) \in S$.
ab) If $t_1, t_2 \in T$ and $t_1 = t_2$ then $\varphi(t_1) = \varphi(t_2)$.

aa) It is clear from the definition that $\varphi(t) \in S$.

ab) To show: If $t_1 = t_2$ then $\varphi(t_1) = \varphi(t_2)$.
Assume $t_1, t_2 \in T$ and $t_1 = t_2$.
Let $s_1, s_2 \in S$ such that $f(s_1) = t_1$ and $f(s_2) = t_2$.
Since $t_1 = t_2$, $f(s_1) = f(s_2)$.
Since f is injective this implies that $s_1 = s_2$.
So $\varphi(t_1) = s_1 = s_2 = \varphi(t_2)$.

So φ is well defined.

b) To show: ba) If $s \in S$ then $\varphi\big(f(s)\big) = s$.
bb) If $t \in T$ then $f\big(\varphi(t)\big) = t$.

ba) This is immediate from the definition of φ.

bb) Assume $t \in T$.
Let $s \in S$ be such that $f(s) = t$.
Then

$$f\big(\varphi(t)\big) = f(s) = t.$$

So $\varphi \circ f$ and $f \circ \varphi$ are the identity functions on S and T respectively.

So φ is an inverse function to f. □

(2.2.7) Proposition.

a) *Let S be a set and let $\sim$ be an equivalence relation on S. The set of equivalence classes of the relation $\sim$ is a partition of S.*

b) *Let S be a set and let $\{S_\alpha\}$ be a partition of S. Then the relation defined by*

$$s \sim t, \text{ if } s, t \text{ are in the same } S_\alpha,$$

is an equivalence relation on S.

Proof.

a) To show: aa) If $s \in S$ then s is in some equivalence class.
ab) If $[s] \cap [t] \neq \emptyset$ then $[s] = [t]$.

aa) Let $s \in S$.
Since $s \sim s$, $s \in [s]$.

ab) Assume $[s] \cap [t] \neq \emptyset$.
To show: $[s] = [t]$.
Since $[s] \cap [t] \neq 0$, there is an $r \in [s] \cap [t]$.
So $s \sim r$ and $r \sim t$.
By transitivity, $s \sim t$.
To show: aba) $[s] \subseteq [t]$
abb) $[t] \subseteq [s]$.

aba) Suppose $u \in [s]$.
Then $u \sim s$.
We know $s \sim t$.
So, by transitivity, $u \sim t$.
Therefore $u \in [t]$.
So $[s] \subseteq [t]$.

abb) Suppose $v \in [t]$.
Then $v \sim t$.
We know $t \sim s$.
So, by transitivity, $v \sim s$.
Therefore $v \in [s]$.
So $[t] \subseteq [s]$.

So $[s] = [t]$.
So the equivalence classes form a partition of S.

b) We must show that $\sim$ is an equivalence relation, i.e. that $\sim$ is reflexive, symmetric, and transitive.
To show: ba) $s \sim s$ for all $s \in S$.
bb) If $s \sim t$ then $t \sim s$.
bc) If $s \sim t$ and $t \sim u$ then $s \sim u$.

ba) s and s are in the same S_α so $s \sim s$.

bb) Assume $s \sim t$.
Then s and t are in the same S_α.
So $t \sim s$.

bc) Assume $s \sim t$ and $t \sim u$.
Then s and t are in the same S_α and t and u are in the same S_α.
So s and u are in the same S_α.
So $s \sim u$.

So $\sim$ is an equivalence relation. $\square$

1. *Let S, T, U be sets and let $f: S \to T$ and $g: T \to U$ be functions.*

a) If f and g are injective then $g \circ f$ is injective.
b) If f and g are surjective then $g \circ f$ is surjective.
c) If f and g are bijective then $g \circ f$ is bijective.

Proof.

a) Assume f and g are injective.
To show: If $s_1, s_2 \in S$ and $(g \circ f)(s_1) = (g \circ f)(s_2)$ then $s_1 = s_2$.
Assume $s_1, s_2 \in S$ and $(g \circ f)(s_1) = (g \circ f)(s_2)$.
Then

$$g\big(f(s_1)\big) = g\big(f(s_2)\big).$$

Thus, since g is injective, $f(s_1) = f(s_2)$.
Thus, since f is injective, $s_1 = s_2$.
So $g \circ f$ is injective.

b) Assume f and g are surjective.
To show: If $u \in U$ then there exists $s \in S$ such that $(g \circ f)(s) = u$.
Assume $u \in U$.
Since g is surjective there exists $t \in T$ such that $g(t) = u$.
Since f is surjective there exists $s \in S$ such that $f(s) = t$.
So

$$\begin{aligned} (g \circ f)(s) &= g\big(f(s)\big) \\ &= g(t) \\ &= u. \end{aligned}$$

So there exists $s \in S$ such that $(g \circ f)(s) = u$.
So $g \circ f$ is surjective.

c) Assume f and g are bijective.
To show: ca) $g \circ f$ is injective.
cb) $g \circ f$ is surjective.

ca) Since f and g are bijective, f and g are injective.
Thus, by a), $g \circ f$ is injective.

cb) Since f and g are bijective, f and g are surjective.
Thus, by b), $g \circ f$ is surjective.

So $g \circ f$ is bijective. $\square$

2. *Let $f: S \to T$ be a function. Then the set $F = \{f^{-1}(t) \mid t \in T\}$ of fibers of the map f is a partition of S.*

Proof.
To show: a) If $s' \in S$ then $s' \in f^{-1}(t)$ for some $t \in T$.
b) If $f^{-1}(t_1) \cap f^{-1}(t_2) \neq \emptyset$ then $f^{-1}(t_1) = f^{-1}(t_2)$.

a) Assume $s' \in S$.
Then $f^{-1}(f(s')) = \{s \in S \mid f(s) = f(s')\}$.
Since $f(s') = f(s')$, $s' \in f^{-1}\big(f(s')\big)$.

b) Assume $f^{-1}(t_1) \cap f^{-1}(t_2) \neq \emptyset$.
Let $s \in f^{-1}(t_1) \cap f^{-1}(t_2)$.
So $f(s) = t_1$ and $f(s) = t_2$.
To show: $f^{-1}(t_1) = f^{-1}(t_2)$.
To show: ba) $f^{-1}(t_1) \subseteq f^{-1}(t_2)$.
bb) $f^{-1}(t_2) \subseteq f^{-1}(t_1)$.

ba) Let $k \in f^{-1}(t_1)$.
Then $f(k) = t_1$
$= f(s)$
$= t_2$.
So $k \in f^{-1}(t_2)$.
So $f^{-1}(t_1) \subseteq f^{-1}(t_2)$.

bb) Let $h \in f^{-1}(t_2)$.
Then $f(k) = t_2$
$= f(s)$
$= t_1$.
So $h \in f^{-1}(t_1)$.
So $f^{-1}(t_2) \subseteq f^{-1}(t_1)$.

So $f^{-1}(t_1) = f^{-1}(t_2)$.

So the set $F = \{f^{-1}(t) \mid t \in T\}$ of fibers of the map f is a partition of S. $\square$

3. *a) Let $f: S \to T$ be a function. Define*

$$\begin{array}{rccc} f'\colon & S & \to & \operatorname{im} f \\ & s & \mapsto & f(s). \end{array}$$

Then the map f' is well defined and surjective.

b) Let $f: S \to T$ be a function and let $F = \{f^{-1}(t) \mid t \in T\}$ be the set of nonempty fibers of f. Define

$$\begin{array}{rccc} \hat{f}\colon & F & \to & T \\ & f^{-1}(t) & \mapsto & t. \end{array}$$

Then the map $\hat{f}$ is well defined and injective.

c) Let $f: S \to T$ be a function and let $F = \{f^{-1}(t) \mid t \in T\}$ be the set of nonempty fibers of f. Define

$$\begin{array}{rccc} \hat{f}'\colon & F & \to & \operatorname{im} f \\ & f^{-1}(t) & \mapsto & t. \end{array}$$

Then the map $\hat{f}'$ is well defined and bijective.

Proof.

a) To show: aa) f' is well defined.
ab) f' is surjective.

aa) To show: aaa) If $s \in S$ then $f'(s) \in \operatorname{im} f$.
aab) If $s_1 = s_2$ then $f'(s_1) = f'(s_2)$.

aaa) Assume $s \in S$.
Then $f'(s) = f(s) \in \operatorname{im} f$ by definition of f' and $\operatorname{im} f$.

aab) Assume $s_1 = s_2$.
Then, by definition of f',

$$f'(s_1) = f(s_1) = f(s_2) = f'(s_2).$$

So f' is well defined.

ab) To show: If $t \in \operatorname{im} f$ then there exists $s \in S$ such that $f'(s) = t$.
Assume $t \in \operatorname{im} f$.
Then $f(s) = t$ for some $s \in S$.
So $f'(s) = f(s) = t$.

So f' is surjective.

b) To show: ba) $\hat{f}$ is well defined.
bb) $\hat{f}$ is injective.

ba) To show: baa) If $f^{-1}(t) \in F$ then $\hat{f}\big(f^{-1}(t)\big) \in T$.
bab) If $f^{-1}(t_1) = f^{-1}(t_2)$ then $\hat{f}\big(f^{-1}(t_1)\big) = \hat{f}\big(f^{-1}(t_2)\big)$.

baa) Assume $f^{-1}(t) \in F$.
Then $\hat{f}\big(f^{-1}(t)\big) = t \in T$, by definition.

bab) Assume $f^{-1}(t_1) = f^{-1}(t_2)$.
Let $s \in f^{-1}(t_1)$.
Then $s \in f^{-1}(t_2)$ also.
So $t_1 = f(s) = t_2$.
Then

$$\hat{f}\big(f^{-1}(t_1)\big) = t_1 = t_2 = \hat{f}\big(f^{-1}(t_2)\big).$$

So $\hat{f}$ is well defined.

bb) To show: If $\hat{f}\big(f^{-1}(t_1)\big) = \hat{f}\big(f^{-1}(t_2)\big)$ then $f^{-1}(t_1) = f^{-1}(t_2)$.
Assume $\hat{f}\big(f^{-1}(t_1)\big) = \hat{f}\big(f^{-1}(t_2)\big)$.
Then $t_1 = t_2$.
To show: $f^{-1}(t_1) = f^{-1}(t_2)$.
This is clearly true since $t_1 = t_2$.
So $\hat{f}$ is injective.

c) By Ex. 2.2.3 b), the function

$$\begin{array}{cccc} \hat{f}\colon & F & \to & T \\ & f^{-1}(t) & \mapsto & t \end{array}$$

is well defined and injective.
By Ex. 2.2.3 a), the function

$$\begin{array}{cccc} \hat{f}'\colon & F & \to & \operatorname{im}\hat{f} \\ & f^{-1}(t) & \mapsto & t \end{array}$$

is well defined and surjective.
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) Assume $t \in \operatorname{im}\hat{f}$.
Then $f^{-1}(t)$ is nonempty.
So there exists $s \in S$ such that $f(s) = t$.
So $t \in \operatorname{im} f$.
So $\operatorname{im}\hat{f} \subseteq \operatorname{im} f$.

cab) Assume $t \in \operatorname{im} f$.
Then there exists $s \in S$ such that $f(s) = t$.
So $f^{-1}(t) \neq \emptyset$.
So $t \in \operatorname{im}\hat{f}$.
So $\operatorname{im} f \subseteq \operatorname{im}\hat{f}$.

So $\operatorname{im}\hat{f} = \operatorname{im} f$.

cb) To show: If $\hat{f}'\big(f^{-1}(t_1)\big) = \hat{f}'\big(f^{-1}t_2)\big)$ then $f^{-1}(t_1) = f^{-1}(t_2)$.
Assume $\hat{f}'\big(f^{-1}(t_1)\big) = \hat{f}'\big(f^{-1}(t_2)\big)$.

So $t_1 = t_2$.
So $f^{-1}(t_1) = f^{-1}(t_2)$.
So $\hat{f}'$ is injective.
So $\hat{f}'$ is well defined and bijective. $\square$

4. *Let S be a set and let $\{0,1\}^S$ be the set of all functions $f\colon S \to \{0,1\}$. Given a subset $T \subseteq S$ define a function $f_T\colon S \to \{0,1\}$ by*

$$f_T(s) = \begin{cases} 0 & \text{if } s \notin T; \\ 1 & \text{if } s \in T. \end{cases}$$

Then the map

$$\begin{array}{cccc} \psi\colon & 2^S & \to & \{0,1\}^S \\ & T & \mapsto & f_T \end{array}$$

is a bijection.

Proof.
To show: a) ψ is well defined.
b) ψ is bijective.
a) To show: aa) If $T \in 2^S$ then $\psi(T) = f_T \in \{0,1\}^S$.
ab) If T_1 and T_2 are subsets of S and $T_1 = T_2$ then $\psi(T_1) = \psi(T_2)$.
aa) It is clear from the definition of f_T that $zz/psi(T) = f_T$ is a function from S to $\{0,1\}$.
ab) Assume T_1 and T_2 are subsets of S and $T_1 = T_2$.
To show: $\psi(T_1) = \psi(T_2)$.
To show: $f_{T_1} = f_{T_2}$.
To show: If $s \in S$ then $f_{T_1}(s) = f_{T_2}(s)$.
Assume $s \in S$.
Case 1: If $s \in T_1$ then, since $T_1 = T_2$, $s \in T_2$.
So

$$f_{T_1}(s) = 1 = f_{T_2}(s).$$

Case 2: If $s \notin T_1$ then, since $T_1 = T_2$, $s \notin T_2$.
So

$$f_{T_1}(s) = 0 = f_{T_2}(s).$$

So $f_{T_1}(s) = f_{T_2}(s)$ for all $s \in S$.
So $f_{T_1} = f_{T_2}$.
So $\psi(T_1) = f_{T_1} = f_{T_2} = \psi(T_2)$.
So ψ is well defined.

b) By virtue of Proposition 2.2.3 we would like to show:
$\psi\colon 2^S \to \{0,1\}^S$ has an inverse function.
Given a function $f\colon S \to \{0,1\}$ define

$$T_f = \{s \in S \mid f(s) = 1\}.$$

Define a function $\varphi\colon \{0,1\}^S \to 2^S$ by

$$\begin{array}{cccc} \varphi\colon & \{0,1\}^S & \to & 2^S \\ & f & \mapsto & T_f. \end{array}$$

To show: ba) φ is well defined.
bb) φ is an inverse function to ψ.

ba) To show: baa) If $f \in \{0,1\}^S$ then $\varphi(f) = T_f \in 2^S$.
bab) If $f_1, f_2 \in \{0,1\}^S$ and $f_1 = f_2$ then

$$\varphi(f_1) = \varphi(f_2).$$

baa) By definition, $T_f = \{s \in S \mid f(s) = 1\}$ is a subset of S.

bab) Assume $f_1, f_2 \in \{0,1\}^S$ and $f_1 = f_2$.
To show: $\varphi(f_1) = \varphi(f_2)$.
To show: $T_{f_1} = T_{f_2}$.
To show: baba) $T_{f_1} \subseteq T_{f_2}$.
babb) $T_{f_2} \subseteq T_{f_1}$.

baba) Assume $s \in T_{f_1}$.
Then $f_1(s) = 1$.
Since $f_2(s) = f_1(s)$, $f_2(s) = 1$.
Thus $s \in T_{f_2}$.
So $T_{f_1} \subseteq T_{f_2}$.

babb) Assume $s \in T_{f_2}$.
Then $f_2(s) = 1$.
Since $f_1(s) = f_2(s)$, $f_1(s) = 1$.
Thus $s \in T_{f_1}$.
So $T_{f_2} \subseteq T_{f_1}$.

So $T_{f_1} = T_{f_2}$.
So $\varphi(f_1) = \varphi(f_2)$.

So φ is well defined.

bb) To show: bba) If $T \in 2^S$ then $\varphi\big(\psi(T)\big) = T$.
bbb) If $f \in \{0,1\}^S$ then $\psi\big(\varphi(f)\big) = f$.

bba) Assume $T \subseteq S$.
To show: $\varphi\big(\psi(T)\big) = T$.
To show: $T_{f_T} = T$.
To show: bbaa) $T_{f_T} \subseteq T$.
bbab) $T \subseteq T_{f_T}$.

bbaa) Assume $t \in T_{f_T}$.
Then $f_T(t) = 1$.
So $t \in T$.
So $T_{f_T} \subseteq T$.

bbab) Assume $t \in T$.
Then $f_T(t) = 1$.
So $t \in T_{f_T}$.
So $T \subseteq T_{f_T}$.

So $T_{f_T} = T$.
So $\varphi\big(\psi(T)\big) = T$.

bbb) Assume $f \in \{0,1\}^S$.
To show: $\psi\big(\varphi(f)\big) = f$.
By definition, $\psi\big(\varphi(f)\big) = f_{T_f}$.
To show: If $s \in S$ then $f_{T_f}(s) = f(s)$.
Assume $s \in S$.

Case 1: $f(s) = 1$.
Then $s \in T_f$.

So $f_{T_f}(s) = 1$.
So $f_{T_f}(s) = f(s)$.

Case 2: $f(s) = 0$.
Then $s \notin T_f$.
So $f_{T_f}(s) = 0$.
So $f_{T_f}(s) = f(s)$.

So $f_{T_f}(s) = f(s)$.

So $\psi\big(\varphi(f)\big) = f$.

So φ is an inverse function to ψ.

So ψ is bijective. $\square$

5. *a) Let $\circ$ be an operation on a set S. If S contains an identity for $\circ$ then it is unique.*
b) Let e be an identity for an associative operation $\circ$ on a set S. Let $s \in S$. If s has an inverse then it is unique.

Proof.

a) Let e, $e' \in S$ be identities for $\circ$.
Then $e \circ e' = e$, since e' is an identity, and $e \circ e' = e'$, since e is an identity.
So $e = e'$.

b) Assume t, $u \in S$ are both inverses for s.
By associativity of $\circ$, $u = (t \circ s) \circ u = t \circ (s \circ u) = t$. $\square$

6. *a) Let S and T be sets and let ι_S and ι_T be the identity maps on S and T respectively.*
For any function $f\colon S \to T$,

$$\iota_T \circ f = f, \qquad \textit{and}$$
$$f \circ \iota_S = f.$$

b) Let $f\colon S \to T$ be a function. If an inverse function to f exists then it is unique.

Proof.

a) Assume $f\colon S \to T$ is a function.
To show: aa) $\iota_T \circ f = f$.
ab) $f \circ \iota_S = f$.
To show: aa) If $s \in S$ then $\iota_T(f(s)) = f(s)$.
ab) If $s \in S$ then $f(\iota_S(s)) = f(s)$.
aa) and ab) follow immediately from the definitions of ι_T and ι_S respectively.

b) Assume φ and ψ are both inverse functions to f.
To show: $\varphi = \psi$.
By the definitions if identity functions and inverse functions,

$$\varphi = \varphi \circ (f \circ \psi) = (\varphi \circ f) \circ \psi = \psi.$$

So, if an inverse function to f exists, then it is unique. $\square$

§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, $g_2 \in G$,*

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

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

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

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

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

So ψ is an inverse function to φ.
So φ is a bijection. $\square$

(1.1.5) Corollary. *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 $\mathrm{Card}(H)$. $\square$

(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. $\square$

(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 $\operatorname{im} f = H$. $\square$

(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. □

§2P. Group Actions

(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 $G_{gs} = gG_sg^{-1}$. $\square$

(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*

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

Proof.
By Proposition 1.2.4, S is a disjoint union of orbits.
So $\mathrm{Card}(S)$ 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*

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

where $| G\colon G_s |$ is the index of $G_s \in G$.

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

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

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 $K = H$. $\square$

(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

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

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. $\square$

(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. $\square$

(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 $s \in Z(g)$. $\square$

(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* $\mathrm{Card}(\mathcal{C}_{g_i})$*. Then*

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

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

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

By Lemma 1.2.14 d) we know that

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

So

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

Chapter 2. RINGS AND MODULES

§1P. Rings

(2.0.4) Proposition. *Let R be a ring and let I be an additive subgroup of R. Then the cosets of I in R partition R.*

Proof.
To show: a) If $r \in R$ then $r \in r' + I$ for some $r' \in R$.
b) If $(r_1 + I) \cap (r_2 + I) \neq \emptyset$ then $r_1 + I = r_2 + I$.

a) Let $r \in R$.
Then $r = r + 0 \in r + I$, since $0 \in I$.
So $r \in r + I$.

b) Assume $(r_1 + I) \cap (r_2 + I) \neq \emptyset$.
To show: ba) $r_1 + I \subseteq r_2 + I$.
bb) $r_2 + I \subseteq r_1 + I$.
Let $s \in (r_1 + I) \cap (r_2 + I)$.
Suppose $s = r_1 + i_1$ and $s = r_2 + i_2$ where $i_1, i_2 \in I$.
Then

$$r_1 = r_1 + i_1 - i_1 = s - i_1 = r_2 + i_2 - i_1 \quad \text{and}$$
$$r_2 = r_2 + i_2 - i_2 = s - i_2 = r_1 + i_1 - i_2.$$

ba) Let $r \in r_1 + I$.
Then $r = r_1 + i$ for some $i \in I$.
Then

$$r = r_1 + i = r_2 + i_2 - i_1 + i \in r_2 + I,$$

since $i_2 - i_1 + i \in I$.
So $r_1 + I \subseteq r_2 + I$.

bb) Let $r \in r_2 + I$.
Then $r = r_2 + i$ for some $i \in I$.
So

$$r = r_2 + i = r_1 + i_1 - i_2 + i \in r_1 + I,$$

since $i_1 - i_2 + i \in I$.
So $r_2 + I \subseteq r_1 + I$.

So $r_1 + I = r_2 + I$.
So the cosets of I in R partition R. □

(2.0.6) Proposition. *Let I be an additive subgroup of a ring R. I is an ideal of R if and only if R/I with operations given by*

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I \quad \textit{and}$$
$$(r_1 + I)(r_2 + I) = r_1 r_2 + I$$

is a ring.

Proof.
$\Longrightarrow$: Assume I is an ideal of R.
To show: a) $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ is a well defined operation on R/I.
b) $(r_1 + I)(r_2 + I) = (r_1 r_2) + I$ is a well defined operation on R/I.
c) $\big((r_1 + I) + (r_2 + I)\big) + (r_3 + I) = (r_1 + I) + \big((r_2 + I) + (r_3 + I)\big)$ for all $r_1 + I, r_2 + I, r_3 + I \in R/I$.
d) $(r_1 + I) + (r_2 + I) = (r_2 + I) + (r_1 + I)$ for all $r_1 + I, r_2 + I \in R/I$.

e) $0 + I = I$ is the zero in R/I.
f) $-r + I$ is the additive inverse of $r + I$.
g) $\big((r_1 + I)(r_2 + I)\big)(r_3 + I) = (r_1 + I)\big((r_2 + I)(r_3 + I)\big)$
for all $r_1 + I, r_2 + I, r_3 + I \in R/I$.
h) $1 + I$ is the identity in R/I.
i) If $r_1 + I$, $r_2 + I$, $r_3 + I \in R/I$ then

$$(r_1 + I)\big((r_2 + I) + (r_3 + I)\big) = (r_1 + I)(r_2 + I) + (r_1 + I)(r_3 + I) \quad \text{and}$$
$$\big((r_2 + I) + (r_3 + I)\big)(r_1 + I) = (r_2 + I)(r_1 + I) + (r_3 + I)(r_1 + I).$$

a) We want the operation on R/I given by

$$\begin{array}{ccc} R/I \times R/I & \to & R/I \\ (r + I, s + I) & \mapsto & (r + s) + I \end{array}$$

to be well defined.
Let $(r_1 + I, s_1 + I), (r_2 + I, s_2 + I) \in R/I \times R/I$ such that
$(r_1 + I, s_1 + I) = (r_2 + I, s_2 + I)$.
Then $r_1 + I = r_2 + I$ and $s_1 + I = s_2 + I$.
To show: $(r_1 + s_1) + I = (r_2 + s_2) + I$.
So we must show: aa) $(r_1 + s_1) + I \subseteq (r_2 + s_2) + I$.
ab) $(r_2 + s_2) + I \subseteq (r_1 + s_1) + I$.

aa) We know $r_1 = r_1 + 0 \in r_2 + I$ since $r_1 + I = r_2 + I$.
So $r_1 = r_2 + k_1$ for some $k_1 \in I$.
Similarly $s_1 = s_2 + k_2$ for some $k_2 \in I$.
Let $t \in (r_1 + s_1) + I$.
Then $t = r_1 + s_1 + k$ for some $k \in I$.
So

$$\begin{aligned} t &= r_1 + s_1 + k \\ &= r_2 + k_1 + s_2 + k_2 + k \\ &= r_2 + s_2 + k_1 + k_2 + k, \end{aligned}$$

since addition is commutative.
So $t = (r_2 + s_2) + (k_1 + k_2 + k) \in r_2 + s_2 + I$.
So $(r_1 + s_1) + I \subseteq (r_2 + s_2) + I$.

ab) Since $r_1 + I = r_2 + I$, we know $r_1 + k_1 = r_2$ for some $k_1 \in I$.
Since $s_1 + I = s_2 + I$, we know $s_1 + k_2 = s_2$ for some $k_2 \in I$.
Let $t \in (r_2 + s_2) + I$.
Then $t = r_2 + s_2 + k$ for some $k \in I$.
So

$$\begin{aligned} t &= r_2 + s_2 + k \\ &= r_1 + k_1 + s_1 + k_2 + k \\ &= r_1 + s_1 + k_1 + k_2 + k, \end{aligned}$$

since addition is commutative.
So $t = (r_1 + s_1) + (k_1 + k_2 + k) \in (r_1 + s_1) + I$.
So $(r_2 + s_2) + I \subseteq (r_1 + s_1) + I$.

So $(r_1 + s_s) + I = (r_2 + s_2) + I$.
So the operation given by $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ is a well defined operation on R/I.

b) We want the operation on R/I given by

$$\begin{array}{rcl} R/I \times R/I & \to & R/I \\ (r+I, s+I) & \mapsto & (rs)+I \end{array}$$

to be well defined.
Let $(r_1 + I, s_1 + I), (r_2 + I, s_2 + I) \in R/I \times R/I$ such that
$(r_1 + I, s_1 + I) = (r_2 + I, s_2 + I)$.
Then $r_1 + I = r_2 + I$ and $s_2 + I = s_2 + I$.
To show: $r_1 s_1 + I = r_2 s_2 + I$.

So we must show: ba) $r_1 s_1 + I \subseteq r_2 s_2 + I$.
bb) $r_2 s_2 + I \subseteq r_1 s_1 + I$.

ba) Since $r_1 + I = r_2 + I$, we know $r_1 = r_2 + k_1$ for some $k_1 \in I$.
Since $s_1 + I = s_2 + I$, we know $s_1 = s_2 + k_2$ for some $k_2 \in I$.
Let $t \in r_1 s_1 + I$.
Then $t = r_1 s_1 + k$ for some $k \in I$.
So

$$\begin{aligned} t &= r_1 s_1 + k \\ &= (r_2 + k_1)(s_2 + k_2) + k \\ &= r_2 s_2 + k_1 s_2 + r_2 k_2 + k_1 k_2 + k, \end{aligned}$$

by using the distributive law.
$k_1 s_2 + r_2 k_2 + k_1 k_2 + k \in I$ by the definition of ideal.
So $t \in r_2 s_2 + I$.
So $r_1 s_1 + I \subseteq r_2 s_2 + I$.

bb) Since $r_1 + I = r_2 + I$, we know $r_1 + k_1 = r_2$ for some $k_1 \in I$.
Since $s_1 + I = s_2 + I$, we know $s_1 + k_2 = s_2$ for some $k_2 \in I$.
Let $t \in r_2 s_2 + I$.
Then $t = r_2 s_2 + k$ for some $k \in I$.
So

$$\begin{aligned} t &= r_2 s_2 + k \\ &= (r_1 + k_1)(s_1 + k_2) + k \\ &= r_1 s_1 + r_1 k_2 + k_1 s_1 + k_1 k_2 + k, \end{aligned}$$

by using the distributive law.
$r_1 k_2 + k_1 s_1 + k_1 k_2 + k \in I$ by the definition of ideal.
So $t \in r_1 s_1 + I$.
So $r_2 s_2 + I \subseteq r_1 s_1 + I$.

So $r_1 s_1 + I = r_2 s_2 + I$.
So the operation given by $(r + I)(s + I) = rs + I$ is a well defined operation on R/I.

c) By the associativity of addition in R and the definition of the operation in R/I,

$$\begin{aligned} \big((r_1 + I) + (r_2 + I)\big) + (r_3 + I) &= \big((r_1 + r_2) + I\big) + (r_3 + I) \\ &= \big((r_1 + r_2) + r_3\big) + I \\ &= \big(r_1 + (r_2 + r_3)\big) + I \\ &= (r_1 + I) + \big((r_2 + r_3) + I\big) \\ &= (r_1 + I) + \big((r_2 + I) + (r_3 + I)\big) \end{aligned}$$

for all $r_1 + I, r_2 + I, r_3 + I \in R/I$.

d) By the commutativity of addition in R and the definition of the operation in R/I,

$$\begin{aligned}(r_1+I)+(r_2+I)&=(r_1+r_2)+I\\&=(r_2+r_1)+I\\&=(r_2+I)+(r_1+I)\end{aligned}$$

for all $r_1+I, r_2+I \in R/I$.

e) The coset $I = 0+I$ is the zero in R/I since

$$\begin{aligned}I+(r+I)&=(0+r)+I\\&=r+I\\&=(r+0)+I=(r+I)+I\end{aligned}$$

for all $r+I \in R/I$.

f) Given any coset $r+I$, its additive inverse is $(-r)+I$ since

$$\begin{aligned}(r+I)+(-r+I)&=r+(-r)+I\\&=0+I\\&=I\\&=(-r+r)+I\\&=(-r+I)+(r+I)\end{aligned}$$

for all $r+I \in R/I$.

g) By the associativity of multiplication in R and the definition of the operation in R/I,

$$\begin{aligned}\big((r_1+I)(r_2+I)\big)(r_3+I)&=(r_1r_2+I)(r_3+I)\\&=(r_1r_2)r_3+I\\&=r_1(r_2r_3)+I\\&=(r_1+I)(r_2r_3+I)\\&=(r_1+I)\big((r_2+I)(r_3+I)\big)\end{aligned}$$

for all $r_1+I, r_2+I, r_3+I \in R/I$.

h) The coset $1+I$ is the identity in R/I since

$$\begin{aligned}(1+I)(r+I)&=1\cdot r+I\\&=r+I\\&=r\cdot 1+I\\&=(r+I)(1+I)\end{aligned}$$

for all $r+I \in R/I$.

i) Assume $r, s, t \in R$. Then by definition of the operations

$$\begin{aligned}(r+I)\big((s+I)+(t+I)\big)&=(r+I)\big((s+t)+I\big)\\&=r(s+t)+I\\&=(rs+rt)+I\\&=(rs+I)+(rt+I)\\&=(r+I)(s+I)+(r+I)(t+I),\end{aligned}$$

and

$$\begin{aligned}\big((s+I)+(t+I)\big)(r+I) &= \big((s+t)+I\big)(r+I)\\ &= (s+t)r+I\\ &= (sr+tr)+I\\ &= (sr+I)+(tr+I)\\ &= (s+I)(r+I)+(t+I)(r+I).\end{aligned}$$

So R/I is a ring.

$\Longleftarrow$: Assume R/I is a ring with operations given by

$$\begin{aligned}(r+I)+(s+I) &= (r+s)+I \quad \text{and}\\ (r+I)(s+I) &= rs+I\end{aligned}$$

for all $r+I, s+I \in R/I$.
To show: If $k \in I$ and $r \in R$ then $kr \in I$ and $rk \in I$.
First we show: If $k \in I$ then $k+I = I$.
To show: a) $k+I \subseteq I$.
b) $I \subseteq k+I$.

a) Let $i \in k+I$.
Then $i = k+k_1$ for some $k_1 \in I$.
Then, since I is a subgroup, $i = k+k_1 \in I$.
So $k+I \subseteq I$.

b) Assume $k_1 \in I$.
Since $k_1 - k \in I$, $k_1 = k+(k_1-k) \in k+I$.
So $I \subseteq k+I$.

Now assume $r \in R$ and $k \in I$.
Then by definition of the operation

$$\begin{aligned}rk+I &= (r+I)(k+I)\\ &= (r+I)I\\ &= (r+I)(0+I)\\ &= 0+I\\ &= I,\end{aligned}$$

and

$$\begin{aligned}kr+I &= (k+I)(r+I)\\ &= (0+I)(r+I)\\ &= 0+I\\ &= I.\end{aligned}$$

So $kr \in I$ and $rk \in I$.
So I is an ideal of R. $\square$

(2.0.9) Proposition. *Let $f\colon R \to S$ be a ring homomorphism. Let 0_R and 0_S be the zeros for R and S respectively. Then*
a) $f(0_R) = 0_S$.
b) For any $r \in R$, $f(-r) = -f(r)$.

Proof.

a) Add $-f(0_R)$ to each side of the following equation.

$$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R).$$

b) Since

$$f(r) + f(-r) = f\big(r + (-r)\big) = f(0_R) = 0_S \quad \text{and}$$
$$f(-r) + f(r) = f\big((-r) + r\big) = f(0_R) = 0_S,$$

then $f(-r) = -f(r)$. □

(2.0.11) Proposition. *Let $f\colon R \to S$ be a ring homomorphism. Then*
a) $\ker f$ *is an ideal of R.*
b) $\operatorname{im} f$ *is a subring of S.*

Proof.

Let 0_R and 0_S be the zeros of R and S respectively.

a) To show: $\ker f$ is an ideal of R.

To show: aa) If $k_1, k_2 \in \ker f$ then $k_1 + k_2 \in \ker f$.
ab) $0_R \in \ker f$.
ac) If $k \in \ker f$ then $-k \in \ker f$.
ad) If $k \in \ker f$ and $r \in R$ then $kr \in \ker f$ and $rk \in \ker f$.

aa) Assume $k_1, k_2 \in \ker f$.
Then $f(k_1) = 0_S$ and $f(k_2) = 0_S$.
So $f(k_1 + k_2) = f(k_1) + f(k_2) = 0_S$.
So $k_1 + k_2 \in \ker f$.

ab) Since $f(0_R) = 0_S$, $0_R \in \ker f$.

ac) Assume $k \in \ker f$.
So $f(k) = 0_S$.
Then

$$f(-k) = -f(k) = 0_S.$$

So $-k \in \ker f$.

ad) Assume $k \in \ker f$ and $r \in R$.
Then

$$f(kr) = f(k)f(r) = 0_S \cdot f(r) = 0_S \quad \text{and}$$
$$f(rk) = f(r)f(k) = f(r) \cdot 0_S = 0_S.$$

So $kr \in \ker f$ and $rk \in \ker f$.

So $\ker f$ is an ideal of R.

b) To show: ba) If $s_1, s_2 \in \operatorname{im} f$ then $s_1 + s_2 \in \operatorname{im} f$.
bb) $0_S \in \operatorname{im} f$.
bc) If $s \in \operatorname{im} f$ then $-s \in \operatorname{im} f$.
bd) If $s_1, s_2 \in \operatorname{im} f$ then $s_1 s_2 \in \operatorname{im} f$.
be) $1_S \in \operatorname{im} f$.

ba) Assume $s_1, s_2 \in \operatorname{im} f$. Then $s_1 = f(r_1)$ and $s_2 = f(r_2)$ for some $r_1, r_2 \in R$.
Then

$$s_1 + s_2 = f(r_1) + f(r_2) = f(r_1 + r_2),$$

since f is a homomorphism.

So $s_1 + s_2 \in \operatorname{im} f$.

bb) By Proposition 2.1.9 a), $f(0_R) = 0_S$, so $0_S \in \operatorname{im} f$.

bc) Assume $s \in \operatorname{im} f$. Then $s = f(r)$ for some $r \in R$.
Then, by Proposition 2.1.9 b),

$$-s = -f(r) = f(-r).$$

So $-s \in \operatorname{im} f$.

bd) Assume $s_1, s_2 \in \operatorname{im} f$. Then $s_1 = f(r_1)$ and $s_2 = f(r_2)$ for some $r_1, r_2 \in R$.
Then

$$s_1 s_2 = f(r_1) f(r_2) = f(r_1 r_2),$$

since f is a homomorphism.
So $s_1 s_2 \in \operatorname{im} f$.

be) By the definition of ring homomorphism, $f(1_R) = 1_S$, so $1_S \in \operatorname{im} f$.

So $\operatorname{im} f$ is a subring of S. $\square$

(2.0.12) Proposition. *Let $f: R \to S$ be a ring homomorphism. Let 0_R be the zero in R. Then*
a) $\ker f = (0_R)$ *if and only if f is injective.*
b) $\operatorname{im} f = S$ *if and only if f is surjective.*

Proof.

a) Let 0_R and 0_S be the zeros in R and S respectively.
$\Longrightarrow$: Assume $\ker f = (0_R)$.
To show: If $f(r_1) = f(r_2)$ then $r_1 = r_2$.
Assume $f(r_1) = f(r_2)$.
Then, by the fact that f is a homomorphism,

$$0_S = f(r_1) - f(r_2) = f(r_1 - r_2).$$

So $r_1 - r_2 \in \ker f$.
But $\ker f = (0_S)$.
So $r_1 - r_2 = 0_R$.
So $r_1 = r_2$.
So f is injective.

$\Longleftarrow$: Assume f is injective.
To show: aa) $(0_R) \subseteq \ker f$.
ab) $\ker f \subseteq (0_R)$.

aa) Since $f(0_R) = 0_S$, $0_R \in \ker f$.
So $(0_R) \subseteq \ker f$.

ab) Let $k \in \ker f$.
Then $f(k) = 0_S$.
So $f(k) = f(0_R)$.
Thus, since f is injective, $k = 0_R$.
So $\ker f \subseteq (0_R)$.

So $\ker f = (0_R)$.

b) $\Longrightarrow$: Assume $\operatorname{im} f = S$.
To show: If $s \in S$ then there exists $r \in R$ such that $f(r) = s$.
Assume $s \in S$.
Then $s \in \operatorname{im} f$.
So there is some $r \in R$ such that $f(r) = s$.
So f is surjective.

$\Longleftarrow$: Assume f is surjective.

To show: a) $\operatorname{im} f \subseteq S$.

b) $S \subseteq \operatorname{im} f$.

a) Let $x \in \operatorname{im} f$.
Then $x = f(r)$ for some $r \in R$.
By the definition of f, $f(r) \in S$.
So $x \in S$.
So $\operatorname{im} f \subseteq S$.

b) Assume $x \in S$.
Since f is surjective there is an r such that $f(r) = x$.
So $x \in \operatorname{im} f$.
So $S \subseteq \operatorname{im} f$.

So $\operatorname{im} f = S$. $\square$

(2.0.13) Theorem.

a) Let $f: R \to S$ be a ring homomorphism and let $K = \ker f$. Define

$$\begin{array}{rccc} \hat{f}: & R/\ker f & \to & S \\ & r + K & \mapsto & f(r). \end{array}$$

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

b) Let $f: R \to S$ be a ring homomorphism and define

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

Then f' is a well defined surjective ring homomorphism.

c) If $f: R \to S$ is a ring homomorphism, then

$$R/\ker f \simeq \operatorname{im} f$$

where the isomorphism is a ring isomorphism.

Proof.

Let 1_R and 1_S be the identities in R and S respectively.

a) To show: aa) $\hat{f}$ is well defined.

ab) $\hat{f}$ is injective.

ac) $\hat{f}$ is a ring homomorphism.

aa) To show: aaa) If $r \in R$ then $\hat{f}(r + K) \in S$.

aab) If $r_1 + K = r_2 + K \in R/K$ then $\hat{f}(r_1 + K) = \hat{f}(r_2 + K)$.

aaa) Assume $r \in R$.
Then $\hat{f}(r + K) = f(r)$, and $f(r) \in S$, by the definition of $\hat{f}$ and f.

aab) Assume $r_1 + K = r_2 + K$.
Then $r_1 = r_2 + k$ for some $k \in K$.
To show: $\hat{f}(r_1 + K) = \hat{f}(r_2 + K)$, i.e.,
To show: $f(r_1) = f(r_2)$.
Since $k \in \ker f$, we have $f(k) = 0$ and so

$$f(r_1) = f(r_2 + k) = f(r_2) + f(k) = f(r_2) + 0 = f(r_2).$$

So $\hat{f}(r_1 + K) = \hat{f}(r_2 + K)$.

So $\hat{f}$ is well defined.

ab) To show: If $\hat{f}(r_1 + K) = \hat{f}(r_2 + K)$ then $r_1 + K = r_2 + K$.

Assume $\hat{f}(r_1 + K) = \hat{f}(r_2 + K)$.
Then $f(r_1) = f(r_2)$.
So $f(r_1) - f(r_2) = 0$.
So $f(r_1 - r_2) = 0$.
So $r_1 - r_2 \in \ker f$.
So $r_1 - r_2 = k$, for some $k \in \ker f$.
So $r_1 = r_2 + k$, for some $k \in \ker f$.
To show: aba) $r_1 + K \subseteq r_2 + K$.
abb) $r_2 + K \subseteq r_1 + K$.

aba) Let $r \in r_1 + K$.
Then $r = r_1 + k_1$, for some $k_1 \in K$.
So $r = r_2 + k + k_1 \in r_2 + K$ since $k + k_1 \in K$.
So $r_1 + K \subseteq r_2 + K$.

abb) Let $r \in r_2 + K$.
Then $r = r_2 + k_2$, for some $k_2 \in K$.
So $r = r_2 + k_2 = r_1 - k + k_2 \in r_1 + K$ since $-k + k_2 \in K$.
So $r_2 + K \subseteq r_1 + K$.

So $r_1 + K = r_2 + K$.

So $\hat{f}$ is injective.

ac) To show: aca) If $r_1 + K, r_2 + K \in R/K$
then $\hat{f}\big((r_1 + k) + (r_2 + K)\big) = \hat{f}(r_1 + K) + \hat{f}(r_2 + K)$.
acb) If $r_1 + K, r_2 + K \in R/K$
then $\hat{f}\big((r_1 + K)(r_2 + K)\big) = \hat{f}(r_1 + K)\hat{f}(r_2 + K)$.
acc) $\hat{f}(1_R + K) = 1_S$.

aca) Let $r_1 + K, r_2 + K \in R/K$.
Since f is a homomorphism,

$$\begin{aligned}\hat{f}(r_1 + K) + \hat{f}(r_2 + K) &= f(r_1) + f(r_2) \\ &= f(r_1 + r_2) \\ &= \hat{f}\big((r_1 + r_2) + K\big) \\ &= \hat{f}\big((r_1 + K) + (r_2 + K)\big).\end{aligned}$$

acb) Let $r_1 + K, r_2 + K \in R/K$.
Since f is a homomorphism,

$$\begin{aligned}\hat{f}(r_1 + K)\hat{f}(r_2 + K) &= f(r_1)f(r_2) \\ &= f(r_1 r_2) \\ &= \hat{f}(r_1 r_2 + K) \\ &= \hat{f}\big((r_1 + K)(r_2 + K)\big).\end{aligned}$$

acc) Since f is a homomorphism,

$$\begin{aligned}\hat{f}(1_R + K) &= f(1_R) \\ &= 1_S.\end{aligned}$$

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

So $\hat{f}$ is a well defined injective ring homomorphism.

b) Let 1_R and 1_S be the identities in R and S respectively.
To show: ba) f' is well defined.

bb) f' is surjective.
bc) f' is a ring homomorphism.

ba) and bb) are proved in Ex. 2.2.4 a) and b), Part I.
bc) To show: bca) If $r_1, r_2 \in R$ then $f'(r_1 + r_2) = f'(r_1) + f'(r_2)$.
bcb) If $r_1, r_2 \in R$ then $f'(r_1 r_2) = f'(r_1) f'(r_2)$.
bcc) $f'(1_R) = 1_S$.

bca) Let $r_1, r_2 \in R$.
Then, since f is a homomorphism,

$$f'(r_1 + r_2) = f(r_1 + r_2) = f(r_1) + f(r_2) = f'(r_1) + f'(r_2).$$

bcb) Let $r_1, r_2 \in R$.
Then, since f is a homomorphism,

$$f'(r_1 r_2) = f(r_1 r_2) = f(r_1) f(r_2) = f'(r_1) f'(r_2).$$

bcc) Since f is a homomorphism,

$$f'(1_R) = f(1_R) = 1_S.$$

So f' is a homomorphism.

So f' is a well defined surjective ring homomorphism.

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

$$\begin{array}{rccc} \hat{f}\colon & R/K & \to & S \\ & r + K & \mapsto & f(r) \end{array}$$

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

$$\begin{array}{rccc} \hat{f}'\colon & R/K & \to & \operatorname{im} \hat{f} \\ & r + K & \mapsto & \hat{f}(r + K) = f(r) \end{array}$$

is a well defined surjective ring 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 $s \in \operatorname{im} \hat{f}$.
Then there is some $r + K \in R/K$ such that $\hat{f}(r + K) = s$.
Let $r' \in r + K$.
Then $r' = r + k$ for some $k \in K$.
Then, since f is a homomorphism and $f(k) = 0$,

$$\begin{aligned} f(r') &= f(r + k) \\ &= f(r) + f(k) \\ &= f(r) \\ &= \hat{f}(r + k) \\ &= s. \end{aligned}$$

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

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

cab) Let $s \in \operatorname{im}\hat{f}$.
Then there is some $r \in R$ such that $f(r) = s$.
So $\hat{f}(r+K) = f(r) = s$.
So $s \in \operatorname{im} f$.
So $\operatorname{im} f \subseteq \operatorname{im}\hat{f}$.

So $\operatorname{im} f = \operatorname{im}\hat{f}$.

cb) To show: If $\hat{f}'(r_1+K) = \hat{f}'(r_2+K)$ then $r_1+K = r_2+K$.
Assume $\hat{f}'(r_1+K) = \hat{f}'(r_2+K)$.
Then $\hat{f}(r_1+K) = \hat{f}(r_2+K)$.
Then, since $\hat{f}$ is injective, $r_1+K = r_2+K$.
So $\hat{f}'$ is injective.

Thus we have

$$\begin{array}{rrcl} \hat{f}': & R/K & \to & \operatorname{im} f \\ & r+K & \mapsto & f(r) \end{array}$$

is a well defined bijective ring homomorphism. □

(2.0.17) Proposition. *Let R be a ring. Let 0_R and 1_R be the zero and the identity in R respectivelly.*

a) There is a unique ring homomorphism $\varphi: \mathbb{Z} \to R$ given by

$$\begin{aligned} \varphi(0) &= 0_R, \\ \varphi(m) &= \underbrace{1_R + \cdots + 1_R}_{m \text{ times}}, \quad \textit{and} \\ \varphi(-m) &= -\varphi(m), \end{aligned}$$

for every $m \in \mathbb{Z}$, $m > 0$.

b) $\ker\varphi = n\,\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ where $n = \operatorname{char}(R)$ is the characteristic of the ring R.

Proof.

Let 1_R and 0_R be the identity and zero of the ring R.

a) Define $\varphi: \mathbb{Z} \to R$ by defining, for each $m > 0$, $m \in \mathbb{Z}$,

$$\begin{aligned} \varphi(m) &= \underbrace{1_R + \cdots + 1_R}_{m \text{ times}}, \\ \varphi(-m) &= -\varphi(m), \\ \varphi(0) &= 0_R. \end{aligned}$$

To show: aa) φ is unique.
ab) φ is well defined.
ac) φ is a homomorphism.

aa) To show: If $\varphi': \mathbb{Z} \to R$ is a homomorphism then $\varphi' = \varphi$.
Assume $\varphi': \mathbb{Z} \to R$ is a homomorphism.
To show: If $m \in \mathbb{Z}$ then $\varphi'(m) = \varphi(m)$.
If $m = 1$ then $\varphi'(1) = 1_R = \varphi(1)$.
If $m > 0$ then

$$\varphi'(m) = \varphi'\underbrace{(1 + \cdots + 1)}_{m \text{ times}} = \underbrace{\varphi'(1) + \cdots + \varphi'(1)}_{m \text{ times}} = \underbrace{1_R + \cdots + 1_R}_{m \text{ times}} = \varphi(m).$$

$$\varphi'(-m) = -\varphi'(m) = -\varphi(m) = \varphi(-m).$$

If $m = 0$ then $\varphi'(0) = 0_R = \varphi(0)$.

ab) This is clear from the definitions.

ac) To show: aca) $\varphi(1) = 1_R$.
acb) $\varphi(mn) = \varphi(m)\varphi(n)$.
acc) $\varphi(m+n) = \varphi(m) + \varphi(n)$.

aca) This follows from the definition of φ.

acb) Let $m, n > 0$. Then, by the distributive law,

$$\varphi(m)\varphi(n) = (\underbrace{1 + \cdots + 1}_{m \text{ times}})(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{1 + \cdots + 1}_{mn \text{ times}} = \varphi(mn).$$

$$\begin{aligned}\varphi(m)\varphi(-n) = \varphi(m)\big(-\varphi(n)\big) &= \varphi(m)(-1_R)\varphi(n) = (-1_R)\varphi(m)\varphi(n) \\ &= (-1_R)\varphi(mn) = -\varphi(mn) = \varphi\big(m(-n)\big).\end{aligned}$$

$$\varphi(-m)\varphi(n) = -\varphi(m)\varphi(n) = (-1_R)\varphi(m)\varphi(n) = (-1_R)\varphi(mn) = -\varphi(mn) = \varphi\big((-m)n\big).$$

$$\varphi(-m)\varphi(-n) = (-1_R)\varphi(m)(-1)_R\varphi(n) = \varphi(m)\varphi(n) = \varphi(mn) = \varphi\big((-m)(-n)\big).$$

acc) Let $m, n > 0$.
Then

$$\varphi(m) + \varphi(n) = \underbrace{1 + \cdots + 1}_{m \text{ times}} + \underbrace{1 + \cdots + 1}_{n \text{ times}} = \underbrace{1 + \cdots + 1}_{m+n \text{ times}} = \varphi(m+n).$$

$$\begin{aligned}\varphi(-m) + \varphi(-n) = -\varphi(m) - \varphi(n) &= -\big(\varphi(m) + \varphi(n)\big) = -\varphi(m+n) \\ &= \varphi\big(-(m+n)\big) = \varphi\big((-m) + (-n)\big).\end{aligned}$$

$$\begin{aligned}\text{If } m \geq n,\ \varphi(m) + \varphi(-n) = \varphi(m) - \varphi(n) &= (\underbrace{1 + \cdots + 1}_{m \text{ times}}) - (\underbrace{1 + \cdots + 1}_{n \text{ times}}) \\ &= \underbrace{1 + \cdots + 1}_{m-n \text{ times}} = \varphi(m-n).\end{aligned}$$

$$\begin{aligned}\text{If } m < n,\ \varphi(m) + \varphi(-n) = \varphi(m) - \varphi(n) &= -\big(\varphi(n) - \varphi(m)\big) \\ &= -\varphi(n-m) = \varphi(m-n).\end{aligned}$$

So φ is a homomorphism.

b) Let $n = \mathrm{char}(R)$.
To show: ba) $n\,\mathbb{Z} \subseteq \ker\varphi$.
bb) $\ker\varphi \subseteq n\,\mathbb{Z}$.

First we show $n \in \ker\varphi$.
By the definition of char(R),

$$\varphi(n) = \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} = 0_R.$$

So $n \in \ker\varphi$.

ba) Let $m \in n\,\mathbb{Z}$.

Then $m = nk$ for some $k \in \mathbb{Z}$.
Since φ is a homomorphism,

$$\varphi(m) = \varphi(nk) = \varphi(n)\varphi(k) = 0 \cdot \varphi(k) = 0.$$

So $\varphi(m) \in \ker \varphi$.
So $n\,\mathbb{Z} \subseteq \ker \varphi$.

bb) Let $m \in \ker \varphi$.
Write $m = nr + s$ where $0 \le s < n$ and $r \in \mathbb{Z}$.
Then, since φ is a homomorphism,

$$0_R = \varphi(m) = \varphi(nr + s) = \varphi(n)\varphi(r) + \varphi(s) = 0_R + \varphi(s) = \underbrace{1_R + \cdots + 1_R}_{s \text{ times}}.$$

By definition of $\mathrm{char}(R)$, n is the smallest positive integer such that $\underbrace{1_R + \cdots 1_R}_{n \text{ times}} = 0_R$.

So $s = 0$.
So $m = nr$.
So $m \in n\,\mathbb{Z}$.
So $\ker \varphi \subseteq n\,\mathbb{Z}$.

So $\ker \varphi = n\,\mathbb{Z}$. $\square$

(2.0.21) Proposition. *Every proper ideal I of a ring R is contained in a maximal ideal of R.*

Proof.
The idea is to use Zorn's lemma on the set of proper ideals of R containing I, ordered by inclusion. We will not prove Zorn's lemma, we will assume it. Zorn's lemma is equivalent to the axiom of choice. For a proof see Isaacs book [I].

Zorn's Lemma. *If S is a poset such that every chain in S has an upper bound then S has a maximal element.*

Let S be the set of proper ideals of R containing I, ordered by inclustion.
To show: Given any chain of ideals in S

$$\cdots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$$

there is a proper ideal J of R containing I that contains all the I_k.
Let

$$J = \bigcup_k I_k.$$

To show: a) J is an ideal.
b) J is a proper ideal.

a) To show: aa) If $i, j \in J$ then $i + j \in J$.
ab) If $i \in J$ and $r \in R$ then $ir \in J$ and $ri \in J$.

aa) Assume $i, j \in J$.
Then $i \in I_k$ and $j \in I_{k'}$ for some k and k'.
So either $i, j \in I_k$ or $i, j \in I_{k'}$ since either $I_k \subseteq I_{k'}$ or $I_{k'} \subseteq I_k$.
So either $i + j \in I_k$ or $i + j \in I_{k'}$ since I_k and $I_{k'}$ are ideals.
So

$$i + j \in \bigcup_k I_k = J.$$

ab) Assume $i \in J$ and $r \in R$.

Then $i \in I_k$ for some k.
Since I_k is an ideal, $ri \in I_k$ and $ir \in I_k$.
So

$$ri \in \bigcup_k I_k = J \quad \text{and} \quad ir \in \bigcup_k I_k = J.$$

So J is an ideal.

b) To show: $1 \notin J$.
Since the I_k are all proper ideals, $1 \notin I_k$ for any k.
So

$$1 \notin \bigcup_k I_k = J.$$

So J is a proper ideal of R.

So every chain of proper ideals in R that contain I has an upper bound.
Thus, by Zorn's lemma, the set S of proper ideals containing I has a maximal element.
So I is contained in a maximal ideal. $\square$

(2.2.4) Proposition. *Let M be a left R-module and let N be a subgroup of M. Then the cosets of N in M partition M.*

Proof.

To show: a) If $m \in M$ then $m \in m' + N$ for some $m' \in M$.
b) If $(m_1 + N) \cap (m_2 + N) \neq \emptyset$ then $m_1 + N = m_2 + N$.

a) Let $m \in M$.
Then, since $0 \in N$, $m = m + 0 \in m + N$.
So $m \in m + N$.

b) Assume $(m_1 + N) \cap (m_2 + N) \neq \emptyset$.
To show: ba) $m_1 + N \subseteq m_2 + N$.
bb) $m_2 + N \subseteq m_1 + N$.
Let $a \in (m_1 + N) \cap (m_2 + N)$.
Suppose $a = m_1 + n_1$ and $a = m_2 + n_2$ where $n_1, n_2 \in N$.
Then

$$\begin{aligned} m_1 &= m_1 + n_1 - n_1 = a - n_1 = m_2 + n_2 - n_1 \quad \text{and} \\ m_2 &= m_2 + n_2 - n_2 = a - n_2 = m_1 + n_1 - n_2. \end{aligned}$$

ba) Let $m \in m_1 + N$.
Then $m = m_1 + n$ for some $n \in N$.
Then

$$m = m_1 + n = m_2 + n_2 - n_1 + n \in m_2 + N,$$

since $n_2 - n_1 + n \in N$.
So $m_1 + N \subseteq m_2 + N$.

bb) Let $m \in m_2 + N$.
Then $m = m_2 + n$ for some $n \in N$.
Then

$$m = m_2 + n = m_1 + n_1 - n_2 + n \in m_1 + N,$$

since $n_1 - n_2 + n \in N$.
So $m_2 + N \subseteq m_1 + N$.

So $m_1 + N = m_2 + N$.

So the cosets of N in M partition M. □

(2.2.5) Theorem. *Let N be a subgroup of a left R-module M. Then N is a submodule of M if and only if M/N with the operations given by*

$$\begin{aligned} (m_1 + N) + (m_2 + N) &= (m_1 + m_2) + N, \quad \textit{and} \\ r(m_1 + N) &= rm_1 + N, \end{aligned}$$

is a left R-module.

Proof.

$\Longrightarrow$: Assume N is a submodule of M.

To show: a) $(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N$ is a well defined operation on M/N.
b) The operation given by $r(m + N) = rm + N$ is well defined.
c) $\big((m_1 + N) + (m_2 + N)\big) + (m_3 + N) = (m_1 + N) + \big((m_2 + N) + (m_3 + N)\big)$ for all $m_1 + N, m_2 + N, m_3 + N \in M/N$.
d) $(m_1 + N) + (m_2 + N) = (m_2 + N) + (m_1 + N)$ for all $m_1 + N, m_2 + N \in M/N$.

e) $0 + N = N$ is the zero in M/N.
f) $-m + N$ is the additive inverse of $m + N$.
g) If $r_1, r_2 \in R$ and $m + N \in M/N$, then $r_1\big(r_2(m + N)\big) = (r_1r_2)(m + N)$.
h) If $m + N \in M/N$ then $1(m + N) = m + N$.
i) If $r \in R$ and $m_1 + N, m_2 + N \in M/N$,
then $r\big((m_1 + N) + (m_2 + N)\big) = r(m_1 + N) + r(m_2 + N)$.
j) If $r_1, r_2 \in R$ and $m + N \in M/N$,
then $(r_1 + r_2)(m + N) = r_1(m + N) + r_2(m + N)$.

a) We want the operation on M/N given by

$$\begin{array}{ccc} M/N \times M/N & \to & M/N \\ (m_1 + N, m_2 + N) & \mapsto & (m_1 + m_2) + N \end{array}$$

to be well defined.
Let $(m_1 + N, m_2 + N), (m_3 + N, m_4 + N) \in M/N \times M/N$ such that
$(m_1 + N, m_2 + N) = (m_3 + N, m_4 + N)$.
Then $m_1 + N = m_3 + N$ and $m_2 + N = m_4 + N$.
To show: $(m_1 + m_2) + N = (m_3 + m_4) + N$.
So we must show: aa) $(m_1 + m_2) + N \subseteq (m_3 + m_4) + N$.
ab) $(m_3 + m_4) + N \subseteq (m_1 + m_2) + N$.

aa) We know $m_1 = m_1 + 0 \in m_3 + N$ since $m_1 + N = m_3 + N$.
So $m_1 = m_3 + k_1$ for some $k_1 \in N$.
Similarly $m_2 = m_4 + k_2$ for some $k_2 \in N$.
Let $t \in (m_1 + m_2) + N$.
Then $t = m_1 + m_2 + k$ for some $k \in N$.
So

$$\begin{aligned} t &= m_1 + m_2 + k \\ &= m_3 + k_1 + m_4 + k_2 + k \\ &= m_3 + m_4 + k_1 + k_2 + k, \end{aligned}$$

since addition is commutative.
So $t = (m_3 + m_4) + (k_1 + k_2 + k) \in m_3 + m_4 + N$.
So $(m_1 + m_2) + N \subseteq (m_3 + m_4) + N$.

ab) Since $m_1 + N = m_3 + N$, we know $m_1 + k_1 = m_3$ for some $k_1 \in N$.
Since $m_2 + N = m_4 + N$, we know $m_2 + k_2 = m_4$ for some $k_2 \in N$.
Let $t \in (m_3 + m_4) + N$.
Then $t = m_3 + m_4 + k$ for some $k \in N$.
So

$$\begin{aligned} t &= m_3 + m_4 + k \\ &= m_1 + k_1 + m_2 + k_2 + k \\ &= m_1 + m_2 + k_1 + k_2 + k, \end{aligned}$$

since addition is commutative.
So $t = (m_1 + m_2) + (k_1 + k_2 + k) \in (m_1 + m_2) + N$.
So $(m_3 + m_4) + N \subseteq (m_1 + m_2) + N$.

So $(m_1 + m_2) + N = (m_3 + m_4) + N$.
So the operation given by $(m_1 + N) + (m_3 + N) = (m_1 + m_3) + N$ is a well defined operation on M/N.

b) We want the operation given by

$$\begin{array}{ccc} R \times M/N & \to & M/N \\ (r, m + N) & \mapsto & rm + N \end{array}$$

to be well defined.
Let $(r_1, m_1 + N), (r_2, m_2 + N) \in (R \times M/N)$ such that $(r_1, m_1 + N) = (r_2, m_2 + N)$.
Then $r_1 = r_2$ and $m_1 + N = m_2 + N$.
To show: $r_1 m_1 + N = r_2 m_2 + N$.

To show: ba) $r_1 m_1 + N \subseteq r_2 m_2 + N$.
bb) $r_2 m_2 + N \subseteq r_1 m_1 + N$.

ba) Since $m_1 + N = m_2 + N$, we know $m_1 = m_2 + n_2$ for some $n_2 \in N$.
Let $k \in r_1 m_1 + N$.
Then $k = r_1 m_1 + n$ for some $n \in N$. So

$$\begin{aligned} k &= r_1 m_1 + n \\ &= r_2(m_2 + n_2) + n \\ &= r_2 m_2 + r_2 n_2 + n. \end{aligned}$$

Since N is a submodule, $r_2 n_2 \in N$, and $r_2 n_2 + n \in N$.
So $k = r_2 m_2 + r_2 n_2 + n \in r_2 m_2 + N$.
So $r_1 m_1 + N \subseteq r_2 m_2 + N$.

bb) Since $m_1 + N = m_2 + N$, we know $m_2 = m_1 + n_1$ for some $n_1 \in N$.
Let $k \in r_2 m_2 + N$.
Then $k = r_2 m_2 + n$ for some $n \in N$. So

$$\begin{aligned} k &= r_2 m_2 + n \\ &= r_1(m_1 + n_1) + n \\ &= r_1 m_1 + r_1 n_1 + n. \end{aligned}$$

Since N is a submodule, $r_1 n_1 \in N$, and $r_1 n_1 + n \in N$.
So $k = r_1 m_1 + r_1 n_1 + n \in r_1 m_1 + N$.
So $r_2 m_2 + N \subseteq r_1 m_1 + N$.

So $r_1 m_1 + N = r_2 m_2 + N$.
So the operation is well defined.

c) By the associativity of addition in M and the definition of the operation in M/N,

$$\begin{aligned} \big((m_1 + N) + (m_2 + N)\big) + (m_3 + N) &= \big((m_1 + m_2) + N\big) + (m_3 + N) \\ &= \big((m_1 + m_2) + m_3\big) + N \\ &= \big(m_1 + (m_2 + m_3)\big) + N \\ &= (m_1 + N) + \big((m_2 + m_3) + N\big) \\ &= (m_1 + N) + \big((m_2 + N) + (m_3 + N)\big) \end{aligned}$$

for all $m_1 + N, m_2 + N, m_3 + N \in M/N$.

d) By the commutativity of addition in M and the definition of the operation in M/N,

$$\begin{aligned} (m_1 + N) + (m_2 + N) &= (m_1 + m_2) + N \\ &= (m_2 + m_1) + N \\ &= (m_2 + N) + (m_1 + N). \end{aligned}$$

for all $m_1 + N, m_2 + N \in M/N$.

e) The coset $N = 0 + N$ is the zero in M/N since

$$
\begin{aligned}
N + (m+N) &= (0+m)+N \\
&= m+N \\
&= (m+0)+N = (m+N)+N
\end{aligned}
$$

for all $m + N \in M/N$.

f) Given any coset $m + N$, its additive inverse is $(-m) + N$ since

$$
\begin{aligned}
(m+N)+(-m+N) &= m+(-m)+N \\
&= 0+N \\
&= N \\
&= (-m+m)+N \\
&= (-m+N)+(m+N)
\end{aligned}
$$

for all $m + N \in M/N$.

g) Assume $r_1, r_2 \in R$ and $m + N \in M/N$.
Then, by definition of the operation,

$$
\begin{aligned}
r_1\big(r_2(m+N)\big) &= r_1(r_2 m + N) \\
&= r_1(r_2 m) + N \\
&= (r_1 r_2)m + N \\
&= (r_1 r_2)(m+N).
\end{aligned}
$$

h) Assume $m + N \in M/N$.
Then, by definition of the operation,

$$
\begin{aligned}
1(m+N) &= (1m)+N \\
&= m+N.
\end{aligned}
$$

i) Assume $r \in R$ and $m_1 + N, m_2 + N \in M/N$.
Then

$$
\begin{aligned}
r\big((m_1+N)+(m_2+N)\big) &= r\big((m_1+m_2)+N\big) \\
&= r(m_1+m_2)+N \\
&= (rm_1+rm_2)+N \\
&= (rm_1+N)+(rm_2+N) \\
&= r(m_1+N)+r(m_2+N).
\end{aligned}
$$

j) Assume $r_1, r_2 \in R$ and $m + N \in M/N$.
Then

$$
\begin{aligned}
(r_1+r_2)(m+N) &= \big((r_1+r_2)m\big)+N \\
&= (r_1 m + r_2 m)+N \\
&= (r_1 m + N)+(r_2 m + N) \\
&= r_1(m+N)+r_2(m+N).
\end{aligned}
$$

So M/N is a left R-module.

$\Longleftarrow$: Assume N is a subgroup of M and (M/N) is a left R-module with action given by $r(m+N) = rm + N$.
To show: N is a submodule of M.

To show: If $r \in R$ and $n \in N$ then $rn \in N$.

First we show: If $n \in N$ then $n + N = N$.

To show: a) $n + N \subseteq N$.
b) $N \subseteq n + N$.

a) Let $k \in n + N$.
So $k = n + n_1$ for some $n_1 \in N$.
Since N is a subgroup, $k = n + n_1 \in N$.
So $n + N \subseteq N$.

b) Let $k \in N$.
Since $k - n \in N$, $k = n + (k - n) \in n + N$.
So $N \subseteq n + N$.

Now assume $r \in R$ and $n \in N$.
Then, by definition of the R-action on M/N,

$$\begin{aligned} rn + N &= r(n + N) \\ &= r(0 + N) \\ &= r \cdot 0 + N \\ &= 0 + N \\ &= N. \end{aligned}$$

So $rn = rn + 0 \in N$.

So N is a submodule of M. □

(2.2.9) Proposition. *Let $f : M \to N$ be an R-module homomorphism. Then*
a) $\ker f$ *is a submodule of* M*.*
b) $\operatorname{im} f$ *is a submodule of* N*.*

Proof.

a) By condition a) in the definition of R-module homomorphism, f is a group homomorphism.
By Proposition 1.1.13 a), $\ker f$ is a subgroup of M.
To show: If $r \in R$ and $k \in \ker f$ then $rk \in \ker f$.
Assume $r \in R$ and $k \in \ker f$.
Then, by the definition of R-module homomorphism,

$$f(rk) = rf(k) = r \cdot 0 = 0.$$

So $rk \in \ker f$.
So $\ker f$ is a submodule of M.

b) By condition a) in the definition of R-module homomorphism, f is a group homomorphism.
By Proposition 1.1.13 b), $\operatorname{im} f$ is a subgroup of N.
To show: If $r \in R$ and $a \in \operatorname{im} f$ then $ra \in \operatorname{im} f$.
Assume $r \in R$ and $a \in \operatorname{im} f$.
Then $a = f(m)$ for some $m \in M$.
By the definition of R-module homomorphism,

$$ra = rf(m) = f(rm).$$

So $ra \in \operatorname{im} f$.
So $\operatorname{im} f$ is a submodule of N. □

(2.2.10) Proposition. *Let $f : M \to N$ be an R-module homomorphism. Let 0_M be the zero in M. Then*
a) $\ker f = (0_M)$ *if and only if f is injective.*
b) $\operatorname{im} f = N$ *if and only if f is surjective.*

Proof.

Let 0_M and 0_N be the zeros in M and N respectively.

a) $\Longrightarrow$: Assume $\ker f = (0_M)$.

To show: If $f(m_1) = f(m_2)$ then $m_1 = m_2$.

Assume $f(m_1) = f(m_2)$.

Then, by the fact that f is a homomorphism,

$$0_N = f(m_1) - f(m_2) = f(m_1 - m_2).$$

So $m_1 - m_2 \in \ker f$.

But $\ker f = (0_M)$.

So $m_1 - m_2 = 0_M$.

So $m_1 = m_2$.

So f is injective.

$\Longleftarrow$: Assume f is injective.

To show: aa) $(0_M) \subseteq \ker f$.

ab) $\ker f \subseteq (0_M)$.

aa) Since $f(0_M) = 0_N$, $0_M \in \ker f$.

So $(0_M) \subseteq \ker f$.

ab) Let $k \in \ker f$.

Then $f(k) = 0_N$.

So $f(k) = f(0_M)$.

Thus, since f is injective, $k = 0_M$.

So $\ker f \subseteq (0_M)$.

So $\ker f = (0_M)$.

b) $\Longrightarrow$: Assume $\operatorname{im} f = N$.

To show: If $n \in N$ then there exists $m \in M$ such that $f(m) = n$.

Assume $n \in N$.

Then $n \in \operatorname{im} f$.

So there is some $m \in M$ such that $f(m) = n$.

So f is surjective.

$\Longleftarrow$: Assume f is surjective.

To show: ba) $\operatorname{im} f \subseteq N$.

bb) $N \subseteq \operatorname{im} f$.

ba) Let $x \in \operatorname{im} f$.

Then $x = f(m)$ for some $m \in M$.

By the definition of f, $f(m) \in N$.

So $x \in N$.

So $\operatorname{im} f \subseteq N$.

bb) Assume $x \in N$.

Since f is surjective there is an m such that $f(m) = x$.

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

So $N \subseteq \operatorname{im} f$.

So $\operatorname{im} f = N$. $\square$

(2.2.11) Theorem.

a) Let $f\colon M \to N$ be an R-module homomorphism and let $K = \ker f$. Define

$$\begin{array}{rccc} \hat{f}\colon & M/\ker f & \to & N \\ & m + K & \mapsto & f(m). \end{array}$$

Then $\hat{f}$ is a well defined injective R-module homomorphism.

b) *Let $f: M \to N$ be an R-module homomorphism and define*

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

Then f' is a well defined surjective R-module homomorphism.

c) *If $f: M \to N$ is an R-module homomorphism, then*

$$M/\ker f \simeq \operatorname{im} f$$

where the isomorphism is an R-module isomorphism.

Proof.

a) To show: aa) $\hat{f}$ is well defined.
ab) $\hat{f}$ is injective.
ac) $\hat{f}$ is an R-module homomorphism.

aa) To show: aaa) If $m \in M$ then $\hat{f}(m+K) \in N$.
aab) If $m_1 + K = m_2 + K \in M/K$ then $\hat{f}(m_1+K) = \hat{f}(m_2+K)$.

aaa) Assume $m \in M$.
Then $\hat{f}(m+K) = f(m)$ and $f(m) \in N$, by the definition of $\hat{f}$ and f.

aab) Assume $m_1 + K = m_2 + K$.
Then $m_1 = m_2 + k$, for some $k \in K$.
To show: $\hat{f}(m_1+K) = \hat{f}(m_2+K)$, i.e.,
To show: $f(m_1) = f(m_2)$.
Since $k \in \ker f$, we have $f(k) = 0$ and so

$$f(m_1) = f(m_2+k) = f(m_2) + f(k) = f(m_2).$$

So $\hat{f}(m_1+K) = \hat{f}(m_2+K)$.
So $\hat{f}$ is well defined.

ab) To show: If $\hat{f}(m_1+K) = \hat{f}(m_2+K)$ then $m_1 + K = m_2 + K$.
Assume $\hat{f}(m_1+K) = \hat{f}(m_2+K)$.
Then $f(m_1) = f(m_2)$.
So $f(m_1) - f(m_2) = 0$.
So $f(m_1 - m_2) = 0$.
So $m_1 - m_2 \in \ker f$.
So $m_1 - m_2 = k$, for some $k \in \ker f$.
So $m_1 = m_2 + k$, for some $k \in \ker f$.
To show: aba) $m_1 + K \subseteq m_2 + K$.
abb) $m_2 + K \subseteq m_1 + K$.

aba) Let $m \in m_1 + K$. Then $m = m_1 + k_1$, for some $k_1 \in K$.
So $m = m_2 + k + k_1 \in m_2 + K$, since $k + k_1 \in K$.
So $m_1 + K \subseteq m_2 + K$.

abb) Let $m \in m_2 + K$. Then $m = m_2 + k_2$, for some $k_2 \in K$.
So $m = m_1 - k + k_2 \in m_1 + K$ since $-k + k_2 \in K$.
So $m_2 + K \subseteq m_1 + K$.

So $m_1 + K = m_2 + K$.
So $\hat{f}$ is injective.

ac) To show: aca) If $m_1 + K, m_2 + K \in M/K$
then $\hat{f}(m_1+K) + \hat{f}(m_2+K) = \hat{f}\big((m_1+K) + (m_2+K)\big)$.
acb) If $r \in R$ and $m + K \in M/K$ then $\hat{f}\big(r(m+K)\big) = r\hat{f}(m+K)$.

aca) Let $m_1 + K, m_2 + K \in M/K$.

Since f is a homomorphism,

$$\begin{aligned}\hat{f}(m_1+K)+\hat{f}(m_2+K) &= f(m_1)+f(m_2)\\ &= f(m_1+m_2)\\ &= \hat{f}\big((m_1+m_2)+K\big)\\ &= \hat{f}\big((m_1+K)+(m_2+K)\big).\end{aligned}$$

acb) Let $r \in R$ and $m+K \in M/K$.
Since f is a homomorphism,

$$\begin{aligned}\hat{f}\big(r(m+K)\big) &= \hat{f}(rm+K)\\ &= f(rm)\\ &= rf(m)\\ &= r\hat{f}(m+K).\end{aligned}$$

So $\hat{f}$ is an R-module homomorphism.
So $\hat{f}$ is a well defined injective R-module homomorphism.

b) To show: ba) f' is well defined.
bb) f' is surjective.
bc) f' is an R-module homomorphism.

ba) and bb) are proved in Ex. 2.2.3 a), Part I.

bc) To show: bca) If $m_1, m_2 \in M$ then $f'(m_1+m_2) = f'(m_1)+f'(m_2)$.
bcb) If $r \in R$ and $m \in M$ then $f'(rm) = rf'(m)$.

bca) Let $m_1, m_2 \in M$.
Then, since f is a homomorphism,

$$f'(m_1+m_2) = f(m_1+m_2) = f(m_1)+f(m_2) = f'(m_1)+f'(m_2).$$

bcb) Let $m_1, m_2 \in M$.
Then, since f is an R-module homomorphism,

$$f'(rm) = f(rm) = rf(m) = rf'(m).$$

So f' is an R-module homomorphism.
So f' is a well defined surjective R-module homomorphism.

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

$$\begin{array}{rccc}\hat{f}\colon & M/K & \to & N\\ & m+K & \mapsto & f(m)\end{array}$$

is a well defined injective R-module homomorphism.

By b), the function

$$\begin{array}{rcccc}\hat{f}'\colon & M/K & \to & \operatorname{im}\hat{f} & \\ & m+K & \mapsto & \hat{f}(m+K) & = f(m)\end{array}$$

is a well defined surjective R-module 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 $n \in \operatorname{im} \hat{f}$.

Then there is some $m + K \in M/K$ such that $\hat{f}(m + K) = n$.

Let $m' \in m + K$.

Then $m' = m + k$ for some $k \in K$.

Then, since f is a homomorphism and $f(k) = 0$,

$$\begin{aligned} f(m') &= f(m + k) \\ &= f(m) + f(k) \\ &= f(m) \\ &= \hat{f}(m + k) \\ &= n. \end{aligned}$$

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

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

cab) Let $n \in \operatorname{im} f$.

Then there is some $m \in M$ such that $f(m) = n$.

So $\hat{f}(m + K) = f(m) = n$.

So $n \in \operatorname{im} \hat{f}$.

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

So $\operatorname{im} f = \operatorname{im} \hat{f}$.

cb) To show: If $\hat{f}'(m_1 + K) = \hat{f}'(m_2 + K)$ then $m_1 + K = m_2 + K$.

Assume $\hat{f}'(m_1 + K) = \hat{f}'(m_2 + K)$.

Then $\hat{f}(m_1 + K) = \hat{f}(m_2 + K)$.

Then, since $\hat{f}$ is injective, $m_1 + K = m_2 + K$.

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

Thus we have

$$\begin{array}{rccc} \hat{f}' \colon & M/K & \to & \operatorname{im} f \\ & m + K & \mapsto & f(m) \end{array}$$

is a well defined bijective R-module homomorphism. $\square$

§1P. Fields

(3.1.3) Proposition. *If $f: K \to F$ is a field homomorphism then f is injective.*

Proof.

To show: $f: K \to F$ is injective.

Assume $f: K \to F$ is a field homomorphism.

To show: If $x_1, x_2 \in K$ and $f(x_1) = f(x_2)$ then $x_1 = x_2$.

Assume $x_1, x_2 \in K$ and $f(x_1) = f(x_2)$.

To show: $x_1 = x_2$.

Proof by contradiction: Assume $x_1 \neq x_2$.

Let 0_K and 0_F be the additive identities in K and F respectively.

Let $1_K$and 1_F be the multiplicative identities in K and F respectively.

Then $f(x_1) - f(x_2) = 0_F$ and $x_1 - x_2 \neq 0_K$.

Let $y = (x_1 - x_2)^{-1}$, which exists by property h) in the definition of a field.

Then, since $f: K \to F$ is a homomorphism and $f(x_1) - f(x_2) = 0_F$,

$$\begin{aligned} 1_F = f(1_K) &= f\big((x_1 - x_2)y\big) \\ &= f(x_1 - x_2)f(y) \\ &= \big(f(x_1) - f(x_2)\big)f(y) \\ &= 0_F \cdot f(y) \\ &= 0_F. \end{aligned}$$

This is a contradiction to property g) in the definition of a field.

So $x_1 = x_2$.

So $f: K \to F$ is injective. □

(3.2.4) Proposition. *Let V be a vector space over a field F and let W be a subgroup of V. Then the cosets of W in V partition V.*

Proof.
To show: a) If $v \in V$ then $v \in v' + W$ for some $v' \in V$.
b) If $(v_1 + W) \cap (v_2 + W) \neq \emptyset$ then $v_1 + W = v_2 + W$.

a) Let $v \in V$.
Then, since $0 \in W$, $v = v + 0 \in v + W$.
So $v \in v + W$.

b) Assume $(v_1 + W) \cap (v_2 + W) \neq \emptyset$.
To show: ba) $v_1 + W \subseteq v_2 + W$.
bb) $v_2 + W \subseteq v_1 + W$.
Let $a \in (v_1 + W) \cap (v_2 + W)$.
Suppose $a = v_1 + w_1$ and $a = v_2 + w_2$ where $w_1, w_2 \in W$.
Then

$$v_1 = v_1 + w_1 - w_1 = a - w_1 = v_2 + w_2 - w_1 \quad \text{and}$$
$$v_2 = v_2 + w_2 - w_2 = a - w_2 = v_1 + w_1 - w_2.$$

ba) Let $v \in v_1 + W$.
Then $v = v_1 + w$ for some $w \in W$.
Then

$$v = v_1 + w = v_2 + w_2 - w_1 + w \in v_2 + W,$$

since $w_2 - w_1 + w \in W$.
So $v_1 + W \subseteq v_2 + W$.

bb) Let $v \in v_2 + W$.
Then $v = v_2 + w$ for some $w \in W$.
Then

$$v = v_2 + w = v_1 + w_1 - w_2 + w \in v_1 + W,$$

since $w_1 - w_2 + w \in W$.
So $v_2 + W \subseteq v_1 + W$.

So $v_1 + W = v_2 + W$.
So the cosets of W in V partition V. $\square$

(3.2.5) Theorem. *Let W be a subgroup of a vector space V over a field F. Then W is a subspace of V if and only if V/W with operations given by*

$$(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W, \quad \textit{and}$$
$$c(v + W) = cv + W,$$

is a vector space over F.

Proof.
$\Longrightarrow$: Assume W is a subspace of V.
To show: a) $(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$ is a well defined operation on V/W.
b) The operation given by $c(v + W) = cv + W$ is well defined.
c) $\big((v_1 + W) + (v_2 + W)\big) + (v_3 + W) = (v_1 + W) + \big((v_2 + W) + (v_3 + W)\big)$ for all $v_1 + W, v_2 + W, v_3 + W \in V/W$.
d) $(v_1 + W) + (v_2 + W) = (v_2 + W) + (v_1 + W)$ for all $v_1 + W, v_2 + W \in V/W$.

e) $0 + W = W$ is the zero in V/W.
f) $-v + W$ is the additive inverse of $v + W$.
g) If $c_1, c_2 \in F$ and $v + W \in V/W$, then $c_1\big(c_2(v + W)\big) = (c_1c_2)(v + W)$.
h) If $v + W \in V/W$ then $1(v + W) = v + W$.
i) If $c \in F$ and $v_1 + W, v_2 + W \in V/W$,
then $c\big((v_1 + W) + (v_2 + W)\big) = c(v_1 + W) + c(v_2 + W)$.
j) If $c_1, c_2 \in F$ and $v + W \in V/W$,
then $(c_1 + c_2)(v + W) = c_1(v + W) + c_2(v + W)$.

a) We want the operation on V/W given by

$$\begin{array}{ccc} V/W \times V/W & \to & V/W \\ (v_1 + W, v_2 + W) & \mapsto & (v_1 + v_2) + W \end{array}$$

to be well defined.
Let $(v_1 + W, v_2 + W), (v_3 + W, v_4 + W) \in V/W \times V/W$ such that
$(v_1 + W, v_2 + W) = (v_3 + W, v_4 + W)$.
Then $v_1 + W = v_3 + W$ and $v_2 + W = v_4 + W$.
To show: $(v_1 + v_2) + W = (v_3 + v_4) + W$.
So we must show: aa) $(v_1 + v_2) + W \subseteq (v_3 + v_4) + W$.
ab) $(v_3 + v_4) + W \subseteq (v_1 + v_2) + W$.

aa) We know $v_1 = v_1 + 0 \in v_3 + W$ since $v_1 + W = v_3 + W$.
So $v_1 = v_3 + w_1$ for some $w_1 \in W$.
Similarly $v_2 = v_4 + w_2$ for some $w_2 \in W$.
Let $t \in (v_1 + v_2) + W$.
Then $t = v_1 + v_2 + w$ for some $w \in W$.
So

$$\begin{aligned} t &= v_1 + v_2 + w \\ &= v_3 + w_1 + v_4 + w_2 + w \\ &= v_3 + v_4 + w_1 + w_2 + w, \end{aligned}$$

since addition is commutative.
So $t = (v_3 + v_4) + (w_1 + w_2 + w) \in v_3 + v_4 + W$.
So $(v_1 + v_2) + W \subseteq (v_3 + v_4) + W$.

ab) Since $v_1 + W = v_3 + W$, we know $v_1 + w_1 = v_3$ for some $w_1 \in W$.
Since $v_2 + W = v_4 + W$, we know $v_2 + w_2 = v_4$ for some $w_2 \in W$.
Let $t \in (v_3 + v_4) + W$.
Then $t = v_3 + v_4 + w$ for some $w \in W$.
So

$$\begin{aligned} t &= v_3 + v_4 + w \\ &= v_1 + w_1 + v_2 + w_2 + w \\ &= v_1 + v_2 + w_1 + w_2 + w, \end{aligned}$$

since addition is commutative.
So $t = (v_1 + v_2) + (w_1 + w_2 + w) \in (v_1 + v_2) + W$.
So $(v_3 + v_4) + W \subseteq (v_1 + v_2) + W$.

So $(v_1 + v_2) + W = (v_3 + v_4) + W$.
So the operation given by $(v_1 + W) + (v_3 + W) = (v_1 + v_3) + W$ is a well defined operation on V/W.

b) We want the operation given by

$$\begin{array}{ccc} F \times V/W & \to & V/W \\ (c, v + W) & \mapsto & cv + W \end{array}$$

to be well defined.
Let $(c_1, v_1 + W), (c_2, v_2 + W) \in (F \times V/W)$ such that $(c_1, v_1 + W) = (c_2, v_2 + W)$.
Then $c_1 = c_2$ and $v_1 + W = v_2 + W$.
To show: $c_1 v_1 + W = c_2 v_2 + W$.

To show: ba) $c_1 v_1 + W \subseteq c_2 v_2 + W$.
bb) $c_2 v_2 + W \subseteq c_1 v_1 + W$.

ba) Since $v_1 + W = v_2 + W$, we know $v_1 = v_2 + w_1$ for some $w_1 \in W$.
Let $t \in c_1 v_1 + W$.
Then $t = c_1 v_1 + w$ for some $w \in W$. So

$$\begin{aligned} t &= c_1 v_1 + w \\ &= c_2(v_2 + w_1) + w \\ &= c_2 v_2 + c_2 w_1 + w, \end{aligned}$$

since $c_1 = c_2$.
Since W is a subspace, $c_2 w_1 \in W$, and $c_2 w_1 + w \in W$.
So $t = c_2 v_2 + c_2 w_1 + w \in c_2 v_2 + W$.
So $c_1 v_1 + W \subseteq c_2 v_2 + W$.

bb) Since $v_1 + W = v_2 + W$, we know $v_2 = v_1 + w_2$ for some $w_2 \in W$.
Let $t \in c_2 v_2 + W$.
Then $t = c_2 v_2 + w$ for some $w \in W$. So

$$\begin{aligned} t &= c_2 v_2 + w \\ &= c_1(v_1 + w_2) + w \\ &= c_1 v_1 + c_1 w_2 + w, \end{aligned}$$

since $c_2 = c_1$.
Since W is a subspace, $c_1 w_2 \in W$, and $c_1 w_2 + w \in W$.
So $t = c_1 v_1 + c_1 w_2 + w \in c_1 v_1 + W$.
So $c_2 v_2 + W \subseteq c_1 v_1 + W$.

So $c_1 v_1 + W = c_2 v_2 + W$.
So the operation is well defined.

c) By the associativity of addition in V and the definition of the operation in V/W,

$$\begin{aligned} \big((v_1 + W) + (v_2 + W)\big) + (v_3 + W) &= \big((v_1 + v_2) + W\big) + (v_3 + W) \\ &= \big((v_1 + v_2) + v_3\big) + W \\ &= \big(v_1 + (v_2 + v_3)\big) + W \\ &= (v_1 + W) + \big((v_2 + v_3) + W\big) \\ &= (v_1 + W) + \big((v_2 + W) + (v_3 + W)\big) \end{aligned}$$

for all $v_1 + W, v_2 + W, v_3 + W \in V/W$.

d) By the commutativity of addition in V and the definition of the operation in V/W,

$$\begin{aligned} (v_1 + W) + (v_2 + W) &= (v_1 + v_2) + W \\ &= (v_2 + v_1) + W \\ &= (v_2 + W) + (v_1 + W). \end{aligned}$$

for all $v_1 + W, v_2 + W \in V/W$.

e) The coset $W = 0 + W$ is the zero in V/W since

$$\begin{aligned} W + (v + W) &= (0 + v) + W \\ &= v + W \\ &= (v + 0) + W \\ &= (v + W) + W \end{aligned}$$

for all $v + W \in V/W$.

f) Given any coset $v + W$, its additive inverse is $(-v) + W$ since

$$\begin{aligned} (v + W) + (-v + W) &= v + (-v) + W \\ &= 0 + W \\ &= W \\ &= (-v + v) + W \\ &= (-v + W) + v + W \end{aligned}$$

for all $v + W \in V/W$.

g) Assume $c_1, c_2 \in F$ and $v + W \in V/W$.
Then, by definition of the operation,

$$\begin{aligned} c_1\big(c_2(v + W)\big) &= c_1(c_2 v + W) \\ &= c_1(c_2 v) + W \\ &= (c_1 c_2)v + W \\ &= (c_1 c_2)(v + W). \end{aligned}$$

h) Assume $v + W \in V/W$.
Then, by definition of the operation,

$$\begin{aligned} 1(v + W) &= (1v) + W \\ &= v + W. \end{aligned}$$

i) Assume $c \in F$ and $v_1 + W, v_2 + W \in V/W$.
Then

$$\begin{aligned} c\big((v_1 + W) + (v_2 + W)\big) &= c\big((v_1 + v_2) + W\big) \\ &= c(v_1 + v_2) + W \\ &= (cv_1 + cv_2) + W \\ &= (cv_1 + W) + (cv_2 + W) \\ &= c(v_1 + W) + c(v_2 + W). \end{aligned}$$

j) Assume $c_1, c_2 \in F$ and $v + W \in V/W$.
Then

$$\begin{aligned} (c_1 + c_2)(v + W) &= \big((c_1 + c_2)v\big) + W \\ &= (c_1 v + c_2 v) + W \\ &= (c_1 v + W) + (c_2 v + W) \\ &= c_1(v + W) + c_2(v + W). \end{aligned}$$

So V/W is a vector space over F.

$\Longleftarrow$: Assume W is a subgroup of V and V/W is a vector space over F with action given by

$c(v+W) = cv + W$.
To show: W is a subspace of V.
To show: If $c \in F$ and $w \in W$ then $cw \in W$.
First we show: If $w \in W$ then $w + W = W$.
To show: a) $w + W \subseteq W$.
b) $W \subseteq w + W$.

a) Let $k \in w + W$.
So $k = w + w_1$ for some $w_1 \in W$.
Since W is a subgroup, $w + w_1 \in W$.
So $w + W \subseteq W$.

b) Let $k \in W$.
Since $k - w \in W$, $k = w + (k - w) \in w + W$.
So $W \subseteq w + W$.

Now assume $c \in F$ and $w \in W$.
Then, by definition of the operation on V/W,

$$\begin{aligned} cw + W &= c(w + W) \\ &= c(0 + W) \\ &= c \cdot 0 + W \\ &= 0 + W \\ &= W. \end{aligned}$$

So $cw = cw + 0 \in W$.
So W is a subspace of V. $\square$

(3.2.8) Proposition. *Let $T: V \to W$ be a linear transformation. Let 0_V and 0_W be the zeros for V and W respectively. Then*

a) $T(0_V) = 0_W$.
b) For any $v \in V$, $T(-v) = -T(v)$.

Proof.

a) Add $-T(0_V)$ to both sides of the following equation.

$$T(0_V) = T(0_V + 0_V) = T(0_V) + T(0_V).$$

b) Since $T(v) + T(-v) = T\big(v + (-v)\big) = T(0_V) = 0_W$ and
$T(-v) + T(v) = T\big((-v) + v\big) + T(0_V) = 0_W$, then

$$-T(v) = T(-v). \quad \square$$

(3.2.10) Proposition. *Let $T: V \to W$ be a linear transformation. Then*

a) $\ker T$ is a subspace of V.
b) $\operatorname{im} T$ is a subspace of W.

Proof.

a) By condition a) in the definition of linear transformation, T is a group homomorphism.
By Proposition 1.1.13 a), $\ker T$ is a subgroup of V.
To show: If $c \in F$ and $k \in \ker T$ then $ck \in \ker T$.
Assume $c \in F$ and $k \in \ker T$.
Then, by the definition of linear transformation,

$$T(ck) = cT(k) = c \cdot 0 = 0.$$

So $ck \in \ker T$.

So $\ker T$ is a subspace of V.

b) By condition a) in the definition of linear transformation, T is a group homomorphism.
By Proposition 1.1.13 b), $\operatorname{im} T$ is a subgroup of W.
To show: If $c \in F$ and $a \in \operatorname{im} T$ then $ca \in \operatorname{im} T$.
Assume $c \in F$ and $c \in \operatorname{im} T$.
Then $a = T(v)$ for some $v \in V$.
By the definition of linear transformation,

$$ca = cT(v) = T(cv).$$

So $ca \in \operatorname{im} T$.
So $\operatorname{im} T$ is a subspace of W. $\square$

(3.2.11) Proposition. *Let $T: V \to W$ be a linear transformation. Let 0_V be the zero in V. Then*

a) $\ker T = (0_V)$ if and only if T is injective.

b) $\operatorname{im} T = W$ if and only if T is surjective.

Proof.

Let 0_V and 0_W be the zeros in V and W respectively.

a) $\Longrightarrow$: Assume $\ker T = (0_V)$.
To show: If $T(v_1) = T(v_2)$ then $v_1 = v_2$.
Assume $T(v_1) = T(v_2)$.
Then, by the fact that T is a homomorphism,

$$0_W = T(v_1) - T(v_2) = T(v_1 - v_2).$$

So $v_1 - v_2 \in \ker T$.
But $\ker T = (0_V)$.
So $v_1 - v_2 = 0_V$.
So $v_1 = v_2$.
So T is injective.

$\Longleftarrow$: Assume T is injective.
To show: aa) $(0_V) \subseteq \ker T$.
ab) $\ker T \subseteq (0_V)$.

aa) Since $T(0_V) = 0_W$, $0_V \in \ker T$.
So $(0_V) \subseteq \ker T$.

ab) Let $k \in \ker T$.
Then $T(k) = 0_W$.
So $T(k) = T(0_V)$.
Thus, since T is injective, $k = 0_V$.
So $\ker T \subseteq (0_V)$.

So $\ker T = (0_V)$.

b) $\Longrightarrow$: Assume $\operatorname{im} T = W$.
To show: If $w \in W$ then there exists $v \in V$ such that $T(v) = w$.
Assume $w \in W$.
Then $w \in \operatorname{im} T$.
So there is some $v \in V$ such that $T(v) = w$.
So T is surjective.

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

ba) Let $x \in \operatorname{im} T$.
Then $x = T(v)$ for some $v \in V$.

By the definition of T, $T(v) \in W$.
So $x \in W$.
So $\operatorname{im} T \subseteq W$.

bb) Assume $x \in W$.
Since T is surjective there is a v such that $T(v) = x$.
So $x \in \operatorname{im} T$.
So $W \subseteq \operatorname{im} T$.

So $\operatorname{im} T = W$. $\square$

(3.2.12) Theorem.

a) Let $T: V \to W$ be a linear transformation and let $K = \ker T$. Define

$$\begin{array}{rccc} \hat{T}\colon & V/\ker T & \to & W \\ & v + K & \mapsto & T(v). \end{array}$$

Then $\hat{T}$ is a well defined injective linear transformation.

b) Let $T: V \to W$ be a linear transformation and define

$$\begin{array}{rccc} T'\colon & V & \to & \operatorname{im} T \\ & v & \mapsto & T(v). \end{array}$$

Then T' is a well defined surjective linear transformation.

c) If $T: V \to W$ is a linear transformation, then

$$V/\ker T \simeq \operatorname{im} T$$

where the isomorphism is a vector space isomorphism.

Proof.

a) To show: aa) $\hat{T}$ is well defined.
ab) $\hat{T}$ is injective.
ac) $\hat{T}$ is a linear transformation.

aa) To show: aaa) If $v \in V$ then $\hat{T}(v + K) \in W$.
aab) If $v_1 + K = v_2 + K \in V/K$ then $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$.

aaa) Assume $v \in V$.
Then $\hat{T}(v + K) = T(v)$ and $T(v) \in W$, by the definition of $\hat{T}$ and T.

aab) Assume $v_1 + K = v_2 + K$.
Then $v_1 = v_2 + K$, for some $k \in K$.
To show: $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$, i.e.,
To show: $T(v_1) = T(v_2)$.
Since $K \in \ker T$, we have $T(k) = 0$ and so

$$T(v_1) = T(v_2 + k) = T(v_2) + T(k) = T(v_2).$$

So $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$.
So $\hat{T}$ is well defined.

ab) To show: If $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$ then $v_1 + K = v_2 + K$.
Assume $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$. Then $T(v_1) = T(v_2)$.
So $T(v_1) - T(v_2) = 0$.
So $T(v_1 - v_2) = 0$.
So $v_1 - v_2 \in \ker T$.
So $v_1 - v_2 = k$, for some $k \in \ker T$.
So $v_1 = v_2 + k$, for some $k \in \ker T$.

To show: aba) $v_1 + K \subseteq v_2 + K$.
abb) $v_2 + K \subseteq v_1 + K$.

aba) Let $v \in v_1 + K$. Then $v = v_1 + k_1$, for some $k_1 \in K$.
So $v = v_2 + k + k_1 \in v_2 + K$, since $k + k_1 \in K$.
So $v_1 + K \subseteq v_2 + K$.

abb) Let $v \in v_2 + K$. Then $v = v_2 + k_2$, for some $k_2 \in K$.
So $v = v_1 - k + k_2 \in v_1 + K$ since $-k + k_2 \in K$.
So $v_2 + K \subseteq v_1 + K$.

So $v_1 + K = v_2 + K$.

So $\hat{T}$ is injective.

ac) To show: aca) If $v_1 + K, v_2 + K \in V/K$ then $\hat{T}(v_1 + K) + \hat{T}(v_2 + K) = \hat{T}\big((v_1 + K) + (v_2 + K)\big)$.
acb) If $c \in F$ and $v + K \in V/K$ then $\hat{T}\big(c(v + K)\big) = c\hat{T}(v + K)$.

aca) Let $v_1 + K, v_2 + K \in V/K$.
Since T is a homomorphism,

$$\begin{aligned}\hat{T}(v_1 + K) + \hat{T}(v_2 + K) &= T(v_1) + T(v_2) \\ &= T(v_1 + v_2) \\ &= \hat{T}\big((v_1 + v_2) + K\big) \\ &= \hat{T}\big((v_1 + K) + (v_2 + K)\big).\end{aligned}$$

acb) Let $c \in F$ and $v + K \in V/K$.
Since T is a homomorphism,

$$\begin{aligned}\hat{T}\big(c(v + K)\big) &= \hat{T}(cv + K) \\ &= T(cv) \\ &= cT(v) \\ &= c\hat{T}(v + K).\end{aligned}$$

So $\hat{T}$ is a linear transformation.

So $\hat{T}$ is a well defined injective linear transformation.

b) To show: ba) T' is well defined.
bb) T' is surjective.
bc) T' is a linear transformation.

ba) and bb) are proved in Ex. 2.2.3 b), Part I.

bc) To show: bca) If $v_1, v_2 \in V$ then $T'(v_1 + v_2) = T'(v_1) + T'(v_2)$.
bcb) If $c \in F$ and $v \in V$ then $T'(cv) = cT'(v)$.

bca) Let $v_1, v_2 \in V$.
Then, since T is a linear transformation,

$$T'(v_1 + v_2) = T(v_1 + v_2) = T(v_1) + T(v_2) = T'(v_1) + T'(v_2).$$

bcb) Let $v_1, v_2 \in V$.
Then, since T is a linear transformation,

$$T'(cv) = T(cv) = cT(v) = cT'(v).$$

So T' is a linear transformation.

So T' is a well defined surjective linear transformation.

c) Let $K = \ker T$.

By a), the function

$$\begin{array}{rccc} \hat{T}\colon & V/K & \to & W \\ & v+K & \mapsto & T(v) \end{array}$$

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

$$\begin{array}{rcccc} \hat{T}'\colon & V/K & \to & \operatorname{im}\hat{T} & \\ & v+K & \mapsto & \hat{T}(v+K) & = T(v) \end{array}$$

is a well defined surjective linear transformation.
To show: ca) $\operatorname{im}\hat{T} = \operatorname{im}T$.
cb) $\hat{T}'$ is injective.

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

caa) Let $w \in \operatorname{im}\hat{T}$.
Then there is some $v+K \in V/K$ such that $\hat{T}(v+K) = w$.
Let $v' \in v+K$.
Then $v' = v+k$ for some $k \in K$.
Then, since T is a linear transformation and $T(k) = 0$,

$$\begin{aligned} T(v') &= T(v+k) \\ &= T(v) + T(k) \\ &= T(v) \\ &= \hat{T}(v+k) \\ &= w. \end{aligned}$$

So $w \in \operatorname{im}T$.
So $\operatorname{im}\hat{T} \subseteq \operatorname{im}T$.

cab) Let $w \in \operatorname{im}T$.
Then there is some $v \in V$ such that $T(v) = w$.
So $\hat{T}(v+K) = T(v) = w$.
So $w \in \operatorname{im}\hat{T}$.
So $\operatorname{im}T \subseteq \operatorname{im}\hat{T}$.

So $\operatorname{im}T = \operatorname{im}\hat{T}$.

cb) To show: If $\hat{T}'(v_1+K) = \hat{T}'(v_2+K)$ then $v_1+K = v_2+K$.
Assume $\hat{T}'(v_1+K) = \hat{T}'(v_2+K)$.
Then $\hat{T}(v_1+K) = \hat{T}(v_2+K)$.
Then, since $\hat{T}$ is injective, $v_1+K = v_2+K$.
So $\hat{T}'$ is injective.

Thus we have

$$\begin{array}{rccc} \hat{T}'\colon & V/K & \to & \operatorname{im}\hat{T} \\ & v+K & \mapsto & T(v) \end{array}$$

is a well defined bijective linear transformation. $\square$