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: $r_1s_1+I = r_2s_2+I$.

So we must show: ba) $r_1s_1+I \subseteq r_2s_2+I$.
bb) $r_2s_2+I \subseteq r_1s_1+I$.

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 $t \in r_1s_1+I$.
Then $t = r_1s_1+k$ for some $k \in I$.
So

$$\begin{aligned} t &= r_1s_1+k \\ &= (r_2+k_1)(s_2+k_2)+k \\ &= r_2s_2+k_1s_2+r_2k_2+k_1k_2+k, \end{aligned}$$

by using the distributive law.
$k_1s_2+r_2k_2+k_1k_2+k \in I$ by the definition of ideal.
So $t \in r_2s_2+I$.
So $r_1s_1+I \subseteq r_2s_2+I$.

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 $t \in r_2s_2+I$.
Then $t = r_2s_2+k$ for some $k \in I$.
So

$$\begin{aligned} t &= r_2s_2+k \\ &= (r_1+k_1)(s_1+k_2)+k \\ &= r_1s_1+r_1k_2+k_1s_1+k_1k_2+k, \end{aligned}$$

by using the distributive law.
$r_1k_2+k_1s_1+k_1k_2+k \in I$ by the definition of ideal.
So $t \in r_1s_1+I$.
So $r_2s_2+I \subseteq r_1s_1+I$.

So $r_1s_1+I = r_2s_2+I$.
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

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

then $f(-r) = -f(r)$. $\square$

(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

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

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 $f\colon R \to S$ 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.

$\Leftarrow$: 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

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

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

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

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

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,

$$\begin{aligned}\hat{f}(r_1+K)\hat{f}(r_2+K)&=f(r_1)f(r_2)\\&=f(r_1r_2)\\&=\hat{f}(r_1r_2+K)\\&=\hat{f}\big((r_1+K)(r_2+K)\big).\end{aligned}$$

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 $\mathrm{im}\,\hat{f} \subseteq \mathrm{im}\, f$.

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

So $\mathrm{im}\, f = \mathrm{im}\,\hat{f}$.

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

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

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 $\varphi\colon \mathbb{Z} \to R$ 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 $n = \mathrm{char}(R)$ 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 $\varphi\colon \mathbb{Z} \to R$ 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 $\varphi'\colon \mathbb{Z} \to R$ is a homomorphism then $\varphi' = \varphi$.
Assume $\varphi'\colon \mathbb{Z} \to R$ 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 $\mathrm{char}(R)$,

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

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 $0 \leq s < n$ 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

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

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*

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

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: $r_1m_1 + N = r_2m_2 + N$.
To show: ba) $r_1m_1 + N \subseteq r_2m_2 + N$.
bb) $r_2m_2 + N \subseteq r_1m_1 + N$.

ba) Since $m_1 + N = m_2 + N$, we know $m_1 = m_2 + n_2$ for some $n_2 \in N$.
Let $k \in r_1m_1 + N$.
Then $k = r_1m_1 + n$ for some $n \in N$. So

$$\begin{aligned} k &= r_1m_1 + n \\ &= r_2(m_2 + n_2) + n \\ &= r_2m_2 + r_2n_2 + n. \end{aligned}$$

Since N is a submodule, $r_2n_2 \in N$, and $r_2n_2 + n \in N$.
So $k = r_2m_2 + r_2n_2 + n \in r_2m_2 + N$.
So $r_1m_1 + N \subseteq r_2m_2 + N$.

bb) Since $m_1 + N = m_2 + N$, we know $m_2 = m_1 + n_1$ for some $n_1 \in N$.
Let $k \in r_2m_2 + N$.
Then $k = r_2m_2 + n$ for some $n \in N$. So

$$\begin{aligned} k &= r_2m_2 + n \\ &= r_1(m_1 + n_1) + n \\ &= r_1m_1 + r_1n_1 + n. \end{aligned}$$

Since N is a submodule, $r_1n_1 \in N$, and $r_1n_1 + n \in N$.
So $k = r_1m_1 + r_1n_1 + n \in r_1m_1 + N$.
So $r_2m_2 + N \subseteq r_1m_1 + N$.
So $r_1m_1 + N = r_2m_2 + N$.
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,

$$\begin{aligned} r_1\big(r_2(m+N)\big) &= r_1(r_2m+N) \\ &= r_1(r_2m)+N \\ &= (r_1r_2)m+N \\ &= (r_1r_2)(m+N). \end{aligned}$$

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

$$\begin{aligned} (r_1+r_2)(m+N) &= \big((r_1+r_2)m\big)+N \\ &= (r_1m+r_2m)+N \\ &= (r_1m+N)+(r_2m+N) \\ &= r_1(m+N)+r_2(m+N). \end{aligned}$$

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

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

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

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

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