R.5. Proofs: Rings

Proposition R.5.1. — *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 there exists $r' \in R$ such that $r \in r' + I$.
(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. □

Proposition R.5.2. — *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*

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

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) If $r_1 + I, r_2 + I, r_3 + I \in R/I$ then $\big((r_1 + I) + (r_2 + I)\big) + (r_3 + I) = (r_1 + I) + \big((r_2 + I) + (r_3 + I)\big)$
(d) If $r_1 + I, r_2 + I \in R/I$ then $(r_1 + I) + (r_2 + I) = (r_2 + I) + (r_1 + I)$.

(e) $0 + I = I$ is the zero in R/I.
(f) $-r + I$ is the additive inverse of $r + I$.
(g) If $r_1 + I, r_2 + I, r_3 + I \in R/I$ then $\big((r_1 + I)(r_2 + I)\big)(r_3 + I) = (r_1 + I)\big((r_2 + I)(r_3 + I)\big)$.
(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, i.e. a function.
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) Since $r_1 + I = r_2 + I$ then $r_1 = r_1 + 0 \in r_2 + I$
So there exists $k_1 \in I$ such that $r_1 = r_2 + k_1$.
Similarly, there exists $k_2 \in I$ such that $s_1 = s_2 + k_2$.
Let $t \in (r_1 + s_1) + I$.
Then there exists $k \in I$ such that $t = r_1 + s_1 + k$.
So

$$t = r_1 + s_1 + k = r_2 + k_1 + s_2 + k_2 + k = r_2 + s_2 + k_1 + k_2 + k,$$

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 $r_1 + I = r_2 + I$ then there exists $k_1 \in I$ such that $r_1 + k_1 = r_2$.
Since $s_1 + I = s_2 + I$ then there exists $k_2 \in I$ such that $s_1 + k_2 = s_2$.
Let $t \in (r_2 + s_2) + I$.
Then there exists $k \in I$ such that $t = r_2 + s_2 + k$.
So

$$t = r_2 + s_2 + k = r_1 + k_1 + s_1 + k_2 + k = r_1 + s_1 + k_1 + k_2 + k,$$

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

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

to be well defined, i.e. a function.
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 $r_1 + I = r_2 + I$, there exists $k_1 \in I$ such that $r_1 = r_2 + k_1$.
Since $s_1 + I = s_2 + I$, there exists $k_2 \in I$ such that $s_1 = s_2 + k_2$.
Let $t \in r_1s_1 + I$.
Then there exists $k \in I$ such that $t = r_1s_1 + k$.
So

$$t = r_1s_1 + k = (r_2 + k_1)(s_2 + k_2) + k = r_2s_2 + k_1s_2 + r_2k_2 + k_1k_2 + k,$$

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 $r_1 + I = r_2 + I$, there exists $k_1 \in I$ such that $r_1 + k_1 = r_2$.
Since $s_1 + I = s_2 + I$, there exists $k_2 \in I$ such that $s_1 + k_2 = s_2$.
Let $t \in r_2s_2 + I$.
Then there exists $k \in I$ such that $t = r_2s_2 + k$.
So

$$t = r_2s_2 + k = (r_1 + k_1)(s_1 + k_2) + k = r_1s_1 + r_1k_2 + k_1s_1 + k_1k_2 + k,$$

by using the distributive law.
By the definition of ideal, $r_1k_2 + k_1s_1 + k_1k_2 + k \in I$.
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, if $r_1 + I, r_2 + I, r_3 + I \in R/I$ then

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

(d) By the commutativity of addition in R and the definition of the operation in R/I, if $r_1 + I, r_2 + I \in R/I$ then

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

(e) The coset $I = 0 + I$ is the zero in R/I since if $r + I \in R/I$ then

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

(f) Given any coset $r + I$, its additive inverse is $(-r) + I$ since if $r + I \in R/I$ then

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

(g) By the associativity of multiplication in R and the definition of the operation in R/I, if $r_1 + I, r_2 + I, r_3 + I \in R/I$ then

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

(h) The coset $1 + I$ is the identity in R/I since if $r + I \in R/I$ then

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

(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

$$(r + I) + (s + I) = (r + s) + I \quad \text{and} \quad (r + I)(s + I) = rs + I, \qquad \text{for } r + I, s + I \in R/I.$$

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 there exists $k_1 \in I$ such that $i = k + k_1$.
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. □

Proposition R.5.3. — *Let $f : R \to S$ 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) *If $r \in R$ then $f(-r) = -f(r)$.*

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

□

Proposition R.5.4. — *Let $f : R \to S$ be a ring homomorphism. Then*
(a) $\ker f$ *is an ideal of R.*
(b) $\mathrm{im} f$ *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 $s_1, s_2 \in \mathrm{im} f$ then $s_1 + s_2 \in \mathrm{im} f$.
(bb) $0_S \in \mathrm{im} f$.
(bc) If $s \in \mathrm{im} f$ then $-s \in \mathrm{im} f$.
(bd) If $s_1, s_2 \in \mathrm{im} f$ then $s_1 s_2 \in \mathrm{im} f$.
(be) $1_S \in \mathrm{im} f$.

(ba) Assume $s_1, s_2 \in \mathrm{im} f$. 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 $s_1 + s_2 \in \mathrm{im} f$.

(bb) By Proposition R.1.1(a), $f(0_R) = 0_S$.
So $0_S \in \mathrm{im} f$.

(bc) Assume $s \in \mathrm{im} f$. Then $s = f(r)$ for some $r \in R$.
Then, by Proposition R.1.1(b),
$$-s = -f(r) = f(-r).$$
So $-s \in \mathrm{im} f$.

(bd) Assume $s_1, s_2 \in \mathrm{im} f$.
Then there exists $r_1, r_2 \in R$ such that $s_1 = f(r_1)$ and $s_2 = f(r_2)$.
Since f is a homomorphism then
$$s_1 s_2 = f(r_1) f(r_2) = f(r_1 r_2),$$
So $s_1 s_2 \in \mathrm{im} f$.

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

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

□

Proposition R.5.5. — *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) $\mathrm{im} f = S$ *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 $\mathrm{im}\, f = S$.
To show: If $s \in S$ then there exists $r \in R$ such that $f(r) = s$.
Assume $s \in S$.
Then $s \in \mathrm{im} f$.
So there exists $r \in R$ such that $f(r) = s$.
So f is surjective.
$\Longleftarrow$: Assume f is surjective.
To show: (a) $\mathrm{im}\, f \subseteq S$.
(b) $S \subseteq \mathrm{im}\, f$.
(a) Let $x \in \mathrm{im}\, f$.
Then there exists $r \in R$ such that $x = f(r)$.
By the definition of f, $f(r) \in S$.
So $x \in S$.
So $\mathrm{im} f \subseteq S$.
(b) Assume $x \in S$.
Since f is surjective there exists $r \in R$ such that $f(r) = x$.
So $x \in \mathrm{im}\, f$.
So $S \subseteq \mathrm{im}\, f$.
So $\mathrm{im}\, f = S$.

$\square$

Theorem R.5.6. —
(a) *Let $f\colon R \to S$ be a ring homomorphism and let $K = \ker f$. Define*

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

Then $\hat{f}$ is a well defined injective ring homomorphism.
(b) *Let $f\colon R \to S$ be a ring homomorphism and define*

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

Then f' is a well defined surjective ring homomorphism.
(c) *If $f\colon R \to S$ is a ring homomorphism, then*

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

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 there exists $k \in \ker f$ such that $r_1 - r_2 = k$.
So there exists $k \in \ker f$ such that $r_1 = r_2 + k$.
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 there exists $k_1 \in K$ such that $r = r_1 + k_1$.
Since $k + k_1 \in K$ then $r = r_2 + k + k_1 \in r_2 + K$
So $r_1 + K \subseteq r_2 + K$.
(abb) Let $r \in r_2 + K$.
Then there exists $k_2 \in K$ such that $r = r_2 + k_2$, for some $k_2 \in K$.

Since $-k + k_2 \in K$ then $r = r_2 + k_2 = r_1 - k + k_2 \in r_1 + K$.
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,

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

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

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

(acc) Since f is a homomorphism,

$$\hat{f}(1_R + K) = f(1_R) = 1_S.$$

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.FIX THIS UPFIX THIS UP FIX

(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 $f'(r_1r_2) = f'(r_1)f'(r_2)$.
(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,

$$f'(r_1r_2) = f(r_1r_2) = f(r_1)f(r_2) = f'(r_1)f'(r_2).$$

(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: $\operatorname{im}\hat{f} = \operatorname{im} f$.
(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 exists $r+K \in R/K$ such that $\hat{f}(r+K) = s$.
Let $r' \in r+K$.
Then there exists $k \in K$ such that $r' = r+k$.
Since f is a homomorphism and $f(k) = 0$ then

$$f(r') = f(r+k) = f(r) + f(k) = f(r) = \hat{f}(r+k) = s.$$

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 exists $r \in R$ 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 $\hat{f}(r_1+K) = \hat{f}(r_2+K)$.
Since $\hat{f}$ is injective then $r_1+K = r_2+K$.
So $\hat{f}'$ is injective.

Thus

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

is a well defined bijective ring homomorphism.

□

Proposition R.5.7. — *Let R be a ring. Let 0_R and 1_R be the zero and the identity in R respectively.*

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

$$\begin{aligned} \varphi(0) &= 0_R, \\ \varphi(m) &= \underbrace{1_R + \cdots + 1_R}_{m \text{ times}}, \quad \textit{and} \\ \varphi(-m) &= -\varphi(m), \qquad \textit{for } m \in \mathbb{Z}_{>0}. \end{aligned}$$

(b) $\ker\varphi = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ *where* $n = char(R)$ *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 $m \in \mathbb{Z}_{>0}$,

$$\begin{aligned} \varphi(m) &= \underbrace{1_R + \cdots + 1_R}_{m \text{ times}}, \\ \varphi(-m) &= -\varphi(m), \\ \varphi(0) &= 0_R. \end{aligned} \tag{R.5.1}$$

To show: (aa) φ is unique.
(ab) φ is well defined, i.e. a function.
(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) Since $\mathbb{Z} = \mathbb{Z}_{>0} \sqcup \{0\} \sqcup -\mathbb{Z}_{>0}$ and the right hand side of each expression in (R.5.1) is an element of R then φ is a fucntion.

(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

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

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

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

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

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 there exists $k\in\mathbb{Z}$ such that $m=nk$.
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 $m=nr+s$ with $0\leqslant s<n$ 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 $\underbrace{1_R+\cdots1_R}_{n\text{ times}}=0_R$.
So $s=0$.
So $m=nr$.
So $m\in n\mathbb{Z}$.
So $\ker\varphi\subseteq n\mathbb{Z}$.

So $\ker\varphi=n\mathbb{Z}$. □

Proposition R.5.8. — *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 [**Isa**, §11D].

> **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 a chain of ideals in S

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

then there exists 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 there exists k and k' such that $i \in I_k$ and $j \in I_{k'}$.
Since either $I_k \subseteq I_{k'}$ or $I_{k'} \subseteq I_k$ then either $i, j \in I_k$ or $i, j \in I_{k'}$.
Since I_k and $I_{k'}$ are ideals then either $i + j \in I_k$ or $i + j \in I_{k'}$
So

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

(ab) Assume $i \in J$ and $r \in R$.
Then there exists k such that $i \in I_k$.
Since I_k is an ideal then $ri \in I_k$ 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 proper ideals then $1 \notin I_k$.
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. $\square$