§1 11-11

Proposition 1.1
Let $\varphi : R \to S$ be a ring homomorphism.

1. R is commutative implies that $\varphi(R)$ is a commutative ring
2. If R and S have unity 1_R and 1_S and φ is surjective, then $\varphi(1_R) = 1_S$
3. If R is a field, then $\varphi(R) = \{0\}$ or $\varphi(R)$ is a field.

   Proof of 3. We know that $\varphi(R)$ is a commutative subring by (1). Let $a \in \varphi(R)$.

   $\varphi(1_R)$ is the multiplicative identity for $\varphi(R)$ so $a = \varphi(\hat{a})$ for some $\hat{a} \in R$.

   $$a \cdot \varphi(1_R) = \varphi(\hat{a})\varphi(1_R) = \varphi(\hat{a}1_R) = \varphi(\hat{a}) = a$$

   Similarly, $\varphi(1_R)a = a$.

   If $\varphi(x) \neq 0_S$, then $x \neq 0_R$. So $\exists x^{-1} \in R$ such that $xx^{-1} = 1_R$.

   $$\varphi(x) \cdot \varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1_R)$$

   So $\varphi(x^{-1})$ equals $(\varphi(x))^{-1}$.

   Either $\varphi(R) = \{0\}$, or it doesn't.

   If $\varphi(1_R) \neq 0_S$, we are done.

   If $\varphi(1_R) = 0_S$, then $\varphi(R) = \{0\}$ because for each $a \in \varphi(R)$, $a = \varphi(\hat{a})$ for some $\hat{a} \in R$. Therefore:

   $$a = \varphi(\hat{a}) = \varphi(\hat{a}1_R) = \varphi(\hat{a})\varphi(1_R) = a0_S = 0$$

   Recall 1.2. Being a field is a stronger property than being an integral domain. When every element has a multiplicative inverse, it must be an integral domain.

   □

§1.1 Ideals

Definition 1.3. An <u>ideal</u> I in ring R is a subring $I \subset R$ such that if $x \in I$ and $r \in R$, then $xr \in I$ and $rx \in I$.

Example 1.4
$\{0\} \subseteq R$ and $R \subseteq R$ are ideals.

Example 1.5

If $a \in R$ is a commutative ring, then $\langle a \rangle = \{ar : r \in R\}$ is an ideal.

$\langle a \rangle$ is a principal ideal.

Proof.
Prooving that $\langle a \rangle$ is a subring:

$\langle a \rangle$ is non empty because $0 = 0a \in \langle a \rangle$.

$r_1 a, r_2 a \in \langle a \rangle \Rightarrow r_1 a \cdot r_2 a = (r_1 \cdot r_2) a \in \langle a \rangle$.

$(ar_1)(ar_2) = a(r_1 a r_2) = ar_3 \in \langle a \rangle$.

Prooving that $\langle a \rangle$ is an ideal:

$$x \in \langle a \rangle \Rightarrow rx \in \langle a \rangle$$

because $x = as$ for some $s \in R$. Therefore $rx = r(as) = a(rs) \in \langle a \rangle$. □

Theorem 1.6

Every ideal in $\mathbb{Z}$ is $\langle n \rangle$ for some n.

Proposition 1.7

The kernel of a ring homomorphism $\varphi : R \to S$ is an ideal of R.

Proof. $K = \ker(\varphi)$ is an additive subgroup.

We must check that $k \in K \Rightarrow rk \in K$ and $kr \in K$ for all $r \in R$.

$rk \in K$ because $\varphi(rk) = \varphi(r)\varphi(k) = \varphi(r)0 = 0$

$kr \in K$ because $\varphi(kr) = \varphi(k)\varphi(r) = 0\varphi(r) = 0$

□

Theorem 1.8
Let I be an ideal of R. The factor group R/I is a ring with multiplication!

$(a+I)(b+I) = (ab+I)$.

Proof. Check that it is well defined. i.e. that if $a+I = a'+I$ and $b+I = b'+I$, then we need $(a+I)(b+I) = (a'+I)(b'+I)$.

Let $a' = a+\alpha$ where $\alpha \in I$, and let $b' = b+\beta$ where $\beta \in I$. Then:

$$a'b' = (a+\alpha)(b+\beta) = ab + a\beta + \alpha b + \alpha\beta$$

$ab+a\beta+\alpha b+\alpha\beta \in ab+I$ because $a\beta+\alpha b+\alpha\beta \in I$. Therefore $a'b'+I = ab+I$ $\square$

Theorem 1.9 (1st Isomorphism Theorem for Rings)
Let $\varphi : R \to S$ be a homomorphism.

Let $I = \ker(\varphi)$.

Let $\phi : R \to R/I$.

Then there exists $\nu : R/I \to \varphi(R)$ such that $\varphi = \nu \circ \phi$.