1 Homomorphisms of Rings

Just like in groups, we are interested in maps between rings that preserve the operations. Specifically, if $R$ and $S$ are rings, then a function $f : R \to S$ is a ring homomorphism if:

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

and

$$f(r_1 \times r_2) = f(r_1) \times f(r_2),$$

for all $r_1, r_2 \in R$.


Note: We have to check BOTH operations here! The map $f_n : \mathbb{Z} \to \mathbb{Z}$ given by multiplication by $n$ is an additive homomorphism, but not a multiplicative one. Determinant is a multiplicative homomorphism but not an additive one.

A homomorphism which is a bijection is an isomorphism. Just like for groups, we can get some basic facts about homomorphisms pretty easily.

**Theorem 1.** Let $\phi : R \to S$ be a homomorphism.

a.) $\phi(0_R) = 0_S$.

b.) $\phi(-a) = -\phi(a)$

One important thing to note. I did not prove that $\phi(1_R) = \phi(1_S)$. This is because it’s not true!!! This will come up on the homework.

Fact: The composition of two homomorphisms is a homomorphism.

The kernel of a homomorphism $f : R \to S$ is the set $\{r \in R \mid f(r) = 0\}$.

Just like for groups, we consider isomorphic rings to be the same for most purposes. Isomorphisms are just our way of formalizing the idea that “no really, these are the same ring, just written differently”.

Also just like for groups, we have the following facts.

**Theorem 2.** Let $f : R \to S$ be a ring homomorphism.

a.) The set $\text{Im}(f) = f(R) = \{s \in S \mid f(r) = s \text{ for some } r \in R\}$ is a subring of $S$. If $R$ has an identity, then $f(1_R) = 1_{f(R)}$.

b.) The kernel of $f$ is a subring of $R$.

Proof. This is achieved just as for groups. Since we know these are subgroups of $R$ and $S$ (If we forget multiplication), we just have to check that the described subsets are closed under multiplication. If $s_1, s_2 \in \text{Im}(f)$, then let $f(r_1) = s_1$ and $f(r_2) = s_2$. Then $f(r_1 r_2) = s_1 s_2$, so that $s_1 s_2$ is in $\text{Im}(f)$. If $i_1, i_2 \in I$, then $f(i_1 i_2) = f(i_1) f(i_2) = 0 \cdot 0 = 0$, so that $i_1 i_2 \in I$. □

As soon as we start talking about homomorphisms and kernels, you should probably expect that cosets and quotients shouldn’t be too far behind, and you’d be right. So let’s see if we can follow more or less the same outline as before.

**Theorem 3.** Let $f : R \to S$ be a ring homomorphism, with kernel $I$. Then if $f(r) = s$, we have

$$f^{-1}(s) = r + I = \{r + i \mid i \in I\}.$$
Proof. We know that, if we just forget about multiplication for a second, that $f$ is a group homomorphism. That means the preimage of $s$, if we just consider $R$ as a group under addition, is a coset if $I$ in $R$. That is, it must be $r + I$.

Alternatively, let $r' \in f^{-1}(s)$, so that $f(r') = s$. Then $f(r' - r) = f(r') - f(r) = s - s = 0$. Hence $r' - r = i \in I$, and $r' = r + i$. Similarly, $f(r + i) = f(r) + f(i) = f(r) + 0 = s$. Hence the two sets are equal.

In general, for any subring $S \leq R$, define the cosets of $S$ in $R$ to be the sets $r + S$, for any $r \in R$. What’s really nice is that we already know a lot about how these cosets work, because they’re defined solely in terms of the addition on $R$, and $R$ is an abelian group under addition. For example, we know how to describe the cosets of a group in terms of an equivalence relation.

**Theorem 4.** For any subring $S \leq R$, the cosets are the equivalence classes of the equivalence relation $r \sim r'$ iff $r - r' \in S$.

Proof. $(R, +)$ is a group.

So, naturally, the next thing we want to do is try and put an operation on the set of cosets of $S$ in $R$. Specifically, we want to know if we can define:

$$(x + R) + (y + R) = (x + y) + R \quad \text{and} \quad (x + R)(y + R) = xy + R.$$ 

But, the question again is whether these operations are well-defined. Notice, though, that we don’t have to worry about the addition operation being well-defined - every subgroup of an abelian group is normal, so $S \triangleleft R$ as groups, and the addition on cosets of $S$ in $R$ is well-defined.

Let’s think about $\mathbb{Z}[x]$. Two subrings of this ring are: $S_1 =$ the polynomials with zero constant term, and $S_2 =$ constant polynomials.

What do the cosets of $S_1$ look like? Well, $f$ and $g$ are in the same coset iff $f - g$ has zero constant term iff $f$ and $g$ have the same constant term. So the cosets consist of all the things with the same constant term. Is multiplication well-defined on cosets? Well, let’s check. Is $(2 + S_1)(3 + S_1)$ well-defined? (PICK RANDOM TERMS with right constant terms and multiply.)

What are the cosets of $S_2$? Well, $f$ and $g$ are in the same coset iff $f - g$ is constant iff $f - g$ have the same non-constant terms. So each coset consists of all the things with the same non-constant part. Is multiplication well-defined on those cosets? Is $(x + S_2)(x + S_2)$ well-defined?

So again, just being a subring isn’t enough. We need something extra. So what’s the issue here - addition on cosets always makes sense, but multiplication might not always. We said before that being a normal subgroup meant that you were good at pretending to be the identity, because normal subgroups act like the identity when we quotient them out. But, which identity are we talking about? The additive identity. And how do I want the additive identity to act multiplicatively? It should absorb multiplication.

We say a subring $I$ is an *ideal* if, for any $r \in R$ and $i \in I$, $ri \in I$ and $ir \in I$.

**Theorem 5.** Let $I$ be a subring of $R$. The operations on $\{r + I\}$ are well-defined if and only if $ri \in I$ and $ir \in I$ for all $r \in R$, $i \in I$.

Proof. Assume that $I$ has the given property. First, notice that addition in $R/I$ is well-defined as a result of what we know about groups. Since $R$ is an abelian additive group, and $I$ is a subgroup, it is a normal subgroup of $R$, and addition makes sense in $R/I$.

So we just have to check that multiplication is well-defined. That is, if we choose different coset representatives for $r + I$ and $s + I$, do we get the same result when we multiply? So let $r'$ and $s'$
be other representatives of $r + I$ and $s + I$. Then $r' = r + i$ and $s' = s + j$ for some $i, j \in I$. Then by definition,

$$(r' + I)(s' + I) = ((r + i) + I)((s + j) + I) = (rs + is + rj + ij) + I.$$ 

But by assumption, $is \in I$, $rj \in I$, and $ij \in I$, so that

$$(r' + I)(s' + I) = rs + I.$$ 

On the other hand, pick $r \in R$ and $i \in I$. Then, assuming that the operation is well-defined, we know that no matter which way we try and compute

$$(r + I)I,$$

we should get the same answer no matter what. So since

$$(r + I)(0 + I) = 0 + I = I \quad \text{and} \quad (r + I)(i + I) = ri + I,$$

We know that $ri + I = I$, so that $ri \in I$. Similarly, $ir \in I$ as well, so $I$ is an ideal.