0.1 Kernels and Ideals

When we studied groups, we studied structure-preserving maps between groups. Now it is time to study structure-preserving maps between rings.

Definition 0.1 (Ring homomorphisms)**.** Let R, S be a rings and $\varphi : R \to S$. Then φ is a **ring homomorphism** if φ is a group homomorphism: $\varphi(a+b) = \varphi(a) + \varphi(b)$ for $a, b \in R$ and φ is multiplicative: $\varphi(ab) = \varphi(a)\varphi(b)$.

Some authors (e.g. [Jac09]) generally require the following axiom: If additionally both R, S have a unity, then $\varphi(1) = 1$. This stipulation is made in order to ensure that units are mapped onto units.

We also make the definition of a

Definition 0.2 (Kernel)**.** The **kernel** of a ring homomorphism φ is the set

$$\ker \varphi = \{ r \in R : \varphi(r) = 0 \}.$$

Example 0.3. For $n > 0 \in \mathbb{Z}$, there is a canonical group homomorphism $\mathbb{Z} \to \mathbb{Z}_n$ given by $m \mapsto m \pmod n$. Since modular arithmetic is multiplicative, this map is in fact a ring homomorphism. //

Example 0.4. If $n \in \mathbb{Z}$, the map $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ defined by $m \mapsto mx$ is not a ring homomorphism unless $n^2 = n$. However φ_n is always a group homomorphism on the additive group of $\mathbb{Z}$. This example emphasizes the importance of checking the multiplicativity of a map. //

Example 0.5 (Evaluation homomorphism)**.** Let R be a commutative ring with unity, let $r \in R$, and let $\mathrm{eval}_r : R[x] \to R$ denote the mapping $f(x) \mapsto f(r)$. This is called the *evaluation homomorphism* because it simply evaluates the polynomial f at r. We leave it to the reader to check that this is indeed a homomorphism. //

Let us now look at a few properties of ring homomorphisms.

Proposition 0.6. Let R, S be rings and $\varphi : R \to S$ be a homomorphism. Then, $\varphi[R]$ is a subring of S, and $\ker \varphi$ is a subring of R.

Proof. Routine. □

Exercise 0.7. Prove the above proposition.

The fact that $\ker \varphi$ is a subring of R is only part of the story though. If $r \in R$, and $a \in \ker \varphi$, then $\varphi(ra) = \varphi(r)\varphi(a) = 0$, so $ra \in \ker \varphi$ too; similary for ar. Such subrings are given a special name:

Definition 0.8 (Ideal)**.** A(n) (two-sided) **ideal** I of a ring R is a subring of R such that for all $i \in I$ and all $r \in R$, both ri and ir are in R.

Note if we only assume that $ri \in R$ then I is a left ideal, and if only $ir \in R$ we call I a right ideal. So a two-sided ideal is both a left and right ideal. Some authors do define left and right ideals, but their utility is rather limited and so we have chosen to omit them. Nevertheless, the concept of one-sided ideals will be developed in the exercises for the interested reader. Henceforth, whenever we say ideal, we shall mean two-sided ideal as in Definition 0.8.

It would be rather silly to give a name to a concept that doesn't have utility. It turns out the utility of ideals is much like normal subgroups: they help us form quotient rings.

Proposition 0.9 (Existence of quotient rings)**.** Let $I \subseteq R$ be a subring. Then I is an ideal of R if and only if the operation $(a+I)(b+I) := ab + I$ is well-defined. if this operation is well-defined, R/I is a quotient ring with multiplication given by said operation.

Proof. Recall that R/I is denoted to be the set of left cosets of I. We shall denote the left coset $\{ a + i : i \in I \}$ by $a + I$. Clearly R/I is already a quotient group since R is abelian. So all that's left to check is the ring operation. We leave checking that as an exercise. □

Exercise 0.10. Complete the proof of Proposition 0.9.

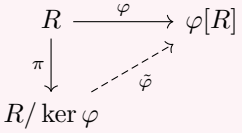
Just like how the study of group homomorphisms is intimately related to the study of normal subgroups, so is the study of ring homomorphisms with the study of ideals.

Proposition 0.11. Every ideal is the kernel of some ring homomorphism

Proof. Consider $r \mapsto r + I$. □

Any time we see quotients, the first isomorphism theorem should come to mind. The reader has probably already formulated the first isomorphism theorem for rings, but we shall state it anyway.

Theorem 0.12 (First Isomorphism Theorem (Rings))**.** Let R, S be rings and let $\varphi : R \to S$ be a ring homomorphism. Then, the map $\tilde{\varphi} : R/\ker\varphi \to \varphi[S]$ given by $\tilde{\varphi}(r \ker\varphi) = \varphi(r)$ is an isomorphism. Diagramatically,



Proof. Exercise. □

Exercise 0.13. Prove Theorem 0.12.

Now that we are sufficiently convinced of the utility of ideals, let's see some examples. In the following examples, notice how we construct homomorphisms to avoid directly arguing that a certain set is an ideal.

Example 0.14. The kernel of any homomorphism is an ideal. Note that Proposition 0.11 shows that these are precisely all the ideals. //

Example 0.15. The trivial ideal $\{0\}$ and the whole ring R are both ideals. This can be done by definition, or by observing that the whole ring R is the kernel of the trivial homomorphism, and the trivial ideal is the kernel of the identity homomorphism $R \to R$. //

Example 0.16 (The ideals of the integers)**.** Let's analyze what the ideals of $\mathbb{Z}$ can be – this will completely characterize *all* homomorphisms out of $\mathbb{Z}$. Of course, we should tackle the easier task first, finding exmaples of ideals of $\mathbb{Z}$. Since the only subgroups of $\mathbb{Z}$ are cyclic of the form $\langle a \rangle$, this severely limits candidates for ideals. We claim these are all in fact ideals. To see this, for each $n > 0$, let ϕ_n be the map $m \mapsto n \mod n$. It's not hard to check that ϕ_n is a ring homomorphism, and that $\ker\phi_n$ is precisely $\langle n \rangle$. So all the ideals of $\mathbb{Z}$ are of the form $\langle n \rangle$.

An alternative argument for this classification is possible by directly using the definition of an ideal and the well-ordering principle; we leave this to the reader. //

Example 0.17 (Kernel of the evaluation homomorphism)**.** We have previously discussed the evaluation homomorphism in a previous example. Let φ denote the evaluation homomorphism from $R[x] \to R$ given by $p(x) \mapsto p(0)$. What is $\ker\varphi$? Well, $\varphi(p) = 0$ if and only if $p(0) = 0$. So the ideal is the set of all polynomials with constant term 0. We will soon introduce notation that will allow us to write this in a cleaner manner. //

0.2 Construction of ideals

We've seen quite a few examples of ideals, but how do we construct ideals? One way is to define ring homomorphisms, and calculate the kernel. However, sometimes this can be annoying. Hence, we shall now introduce some operations which allow us to create ideals. For this section, R will always be a ring with unity.

Definition 0.18 (Ideal generated by a set)**.** Let R be a ring with unity, and let $A \subseteq R$ be *any* subset. Then the **(two-sided) ideal generated by** A, denoted (A), is the smallest (two-sided) ideal of R that contains A. Equivalently, it is the intersection of all the (two-sided) ideals of R that contain A.

If A is finite, i.e. $A = \{a_1, \ldots, a_n\}$, then we can also write $(a_1, \ldots, a_n)$. If A is a single element, i.e. $A = \{a\}$, then we write (a).

If A is finite, then the ideal generated by A is said to be **finitely generated**. If A is a singleton, the ideal generated by A is called a **principal ideal**.

Since the whole ring R is an ideal, the set of ideals containing A is nonempty, and hence the intersection of this set is a well-defined concept. One can also equivalently define the left or right ideal generated by A. We shall shortly see that these are related to the next concept we shall introduce:

Definition 0.19. Let R be a ring and $A \subseteq R$ be *any* set.

Let RA denote the set of all finite R-linear combinations of elements in A, i.e.

$$RA = \left\{ \sum_{\text{finite}} r_i a_i : r_i \in R, a_i \in A \right\}.$$

We can define AR in a similar manner, and RAR would be the set of all finite sums of elements of the form $r_i a_i r_i'$. It turns out