Ring Theory, Part I: Introduction to Rings

Jay Havaldar

Definition: A **ring** R is a set with an addition and a multiplication operation which satisfies the following properties: - R is an abelian group under addition. - Distributivity of addition and multiplication. - There is a multiplicative identity 1. Some authors do not include this property, in which case we have what is called a **rng**.

Note that I denote 0 to be the additive identity, i.e. $r + 0 = 0 + r = 0$ for $r \in R$.

A **commutative ring** has a commutative multiplication operation.

Definition: Suppose $xy = 0$, but $x \neq 0$ and $y \neq 0$. Then x, y are called **zero divisors**.

Definition: A commutative ring without zero divisors, where $1 \neq 0$ (in other words our ring is not the zero ring), is called an **integral domain**.

Definition: A **unit** element in a ring is one that has a multiplicative inverse. The set of all units in a ring is denoted $R^\times$, often called the multiplicative group of R.

Definition: A **field** is a commutative ring in which every nonzero element is a unit.

Examples of rings include: $\mathbb{Z}, End(R, R)$. Examples of integral domains include $\mathbb{Z}$ (hence the name), as well as the ring of complex polynomials. Examples of fields include $\mathbb{Q}, \mathbb{C}, \mathbb{R}$.

Note that not every integral domain is a field, but as we will later show, every field is an integral domain.

Now we can define a fundamental concept of ring theory: ideals, which can be thought of as the analogue of normal groups for rings, in the sense that they serve the same practical role in the isomorphism theorems.

0.1 Ideals and Homomorphisms

Let R be a ring. A **left ideal** J is a subset of R satisfying the following properties: - J is closed under addition. - For every $x \in J$, $r \in R$, we have $rx \in J$

We can change the second property to closure under right multiplication for a right ideal; in the case of commutative rings we just speak of ideals. Note that the second condition guarantees that $0x = 0$ is in every ideal.

Definition: A **ring homomorphism** is a map φ between rings so that: - $\varphi(x + y) = \varphi(x) + \varphi(y)$. - $\varphi(xy) = \varphi(x)\varphi(y)$. - $\varphi(1) = 1$.

In this way, a ring homomorphism preserves structure. Note that an ideal in a ring is automatically a normal subgroup since a ring is an additive abelian group. We can extend this analogy by generalizing fundamental theorems regarding normal groups. We now come to the isomorphism theorems for rings, which are analogues of the same theorems for groups.

0.1.1 Isomorphism Theorems for Rings

First Isomorphism Theorem Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker \varphi$ is an ideal of R, and $\varphi(R)$ is a subring of S. Furthermore:

$$S/\ker\varphi \cong \varphi(R)$$

We can also define a canonical homomorphism $\varphi : R \to R/I$ from R to the ring of representative cosets of I, such that $\varphi : r \mapsto r + I$.

It is not hard to prove that this is a well-defined homomorphism; indeed, this is a homomorphism whose kernel is I. In this way, we show that every ideal is the kernel of a homomorphism, and that every kernel of a homomorphism is an ideal.

Second Isomorphism Theorem Let A be a subring of and B an ideal of R. Then the following set is a subring of R:

$$A + B = \{a + b \mid a \in A, b \in B\}$$

Furthermore, $A \cap B$ is an ideal of A, and finally:

$$(A + B)/B \cong A/(A \cap B)$$

Third Isomorphism Theorem Let I, J be ideals of R, with $I \subseteq J$. Then J/I is an ideal of R/I and:

$$(R/I)/(J/I) \cong R/J$$

We also have an analogue for the correspondence theorem for groups:

Correspondence Theorem for Rings As before, we can construct a bijection from the set of all subrings of R which contain and ideal I, and the subrings of R/I. In particular, the bijection is the map $J \mapsto J/I$, where $I \subseteq J$ and J is a subring of R which contains I.

Example Let $R = C[0, 1]$, the continuous functions defined on the interval $[0, 1]$. Then:

$$I = \left\{ f \in R \mid f(\frac{1}{2}) = 0 \right\}$$

I is an ideal.

Example Let $R = \mathbb{Z}$, the ring of integers. Then, an ideal can be written:

$$I_a = \{na \mid n \in \mathbb{Z}\}$$

Pick any integer a. If an ideal contains a, by multiplicative closure it also contains all the integer multiples of a.

0.2 Properties of Ideals

Let R be a ring and $a \in R$. Then we denote (a) as the **ideal generated by** a. An ideal generated by one element is called **principal ideal**. An ideal generated by a finite set of generators is called a finitely generated ideal. A principal ideal is something like a cyclic group, and a finitely generated ideal is something like a finitely generated subgroup.

Definition: Let I, J be ideals of R. Then we can construct the following ideals:

$$I + J = \{a + b \mid a \in I, b \in J\}$$

$$IJ = \left\{ \sum_{i=1}^{k} ab \mid a \in I, b \in J, k \in \mathbb{Z} \right\}$$

$$I^n = I^{n-1} I$$

Since an ideal contains the additive identity, it is clear that $I + J$ contains both I and J, and indeed it is the smallest ideal which contains both. Also note that IJ must contain the finite sums of elements of the form ab, since without that condition we would not have closure under addition. These constructions will be useful for many later proofs.

Definition: Let R be a commutative ring. P is called a **prime ideal** if $P \neq R$ and whenever $ab \in P$, then $a \in P$ or $b \in P$ (possibly both).

The definition of a prime ideal should look something like the definition of a prime number. If an integer ab divides a prime, then one of the two factors divides the prime. Indeed, (p) is a prime ideal in the integers for any prime p (and 0 is the only other prime ideal).

Proposition Suppose R is a commutative ring. Then P is a prime ideal iff R/P is an integral domain.

Proof: Suppose P is prime. Then $ab = 0$ in R/P iff $ab \in P$ in R. Thus, if R/P is an integral domain, then $ab = 0$ iff $a = 0$ or $b = 0$, or equivalently, $ab \in P$ iff $a \in P$ or $b \in P$. The converse follows similarly.

We will now take a look at the ideal structure of fields.

Proposition Let I be an ideal of R. Then $I = R$ iff I contains a unit.

Proof: If I contains a unit u, then $(ru^{-1})u \in I \implies r \in I$ for any element $r \in R$.

Proposition Let R be a commutative ring. Then R is a field iff its only ideals are 0 and R.

Proof: Suppose R is a field, and thus every non-zero element is a unit. By the previous proposition, every non-zero ideal is R. Conversely, suppose R has no proper non-trivial ideals. Take an arbitrary non-zero element $u \in R$. By hypothesis, $(u) = R$, so in particular $1 = vu$ for some $v \in R$. Thus, R is a field because all its non-zero elements are units.

Corollary If R is a field, then any nonzero ring homomorphism from R into another ring is an injection.

The kernel of any homomorphism is an ideal by the isomorphism theorems; since 0 is the only proper ideal, the kernel of any homomorphism is 0 and we have an injection.

So the ideal structure of fields is fairly simple.

Definition: An ideal M is called a maximal ideal in a ring R if the only ideal properly containing M is R.

Not all rings have maximal ideals. However, we can guarantee their existence by assuming **Zorn's Lemma**, which is equivalent to the controversial axiom of choice. I won't go into the proof here, but note that we don't need to invoke the axiom of choice to guarantee maximal ideals most rings; sometimes the maximal ideals are fairly obvious.

Proposition In a ring with identity every proper ideal is contained in some maximal ideal.

Now, we draw the connection between maximal ideals and fields.

Proposition

Suppose R is a commutative ring. Then M is a maximal ideal in R iff R/M is a field.

Proof: By the correspondence theorem, there is a canonical homomorphism between the ideals of R/M and the ideals of R containing M. It is immediately clear that M is maximal if and only if R/M has no nonzero proper ideals, and is thus a field.

This proposition is crucial, as it allows us to construct fields in rings with maximal ideals simply by taking a quotient with a maximal ideal.

Proposition Assume R is commutative. Every maximal ideal of R is a prime ideal.

Proof: If an ideal is maximal, then R/M is a field. A field is certainly an integral domain, since $xy = 0 \implies x^{-1}xy = 0 \implies y = 0$. Therefore, M is a prime ideal.

We have thus shown that fields are a proper subset of integral domains; and that maximal ideals are proper subsets of prime ideals.

0.3 Quotient Fields

A reasonable question to ask is: how can we turn a (commutative) ring into a field? The simple answer is that we add inverses.

We model our answer after the rational numbers. We define fractions of the form $\frac{a}{b}$, where $a, b \in R$, and say that $\frac{a}{b}$ is equivalent to $\frac{c}{d}$ if $ad = bc$. We define a new ring with the elements being the equivalence classes of such fractions, and it's easy to check that with addition and multiplication as in $\mathbb{Q}$, we nearly have a well-defined ring.

The one issue is that we can't have zero or zero divisors in the denominator, or else we will end up with nonsensical statements like $0 = 1$ To avoid this, we assume R is integral (no zero divisors). It is easy to see then that we have invented a field, called the **quotient field** of R, which we will call K.

Definition: Let R be an integral domain. Then we define Quot(R) to be the field constructed by identifying equivalence classes of pairs (a, b) in R ($b \neq 0$) under the equivalence relation $(a, b)\ (cd) \iff ad = bc$, with the ring structure defined above.

There is a natural map from R into K, so that $r \mapsto \frac{r}{1}$. It is not hard to see that this is an injective ring homomorphism.

Definition: An injective ring homomorphism is called an **embedding**.

Suppose that R is a subring of a field F. Then we can create a field of elements of the form ab^{-1}, where $a, b \in R$ and $b \neq 0$. This is called the quotient field of R in F. This construction is naturally isomorphic to the above quotient field of R, with the isomorphism:

$$a/b \mapsto ab^{-1}$$

An important property of a quotient field is that it is in a way, the smallest field in which we can embed a ring. This is illuminated in the following theorem.

Theorem Let R be an integral ring, and $f : R \to E$ be an embedding of R into some field E. Let K be the quotient field of R.

Then, there is a unique embedding f^* from K to E, such that $f = f$, when restricted to $R \subset K$.

Visually, K, f^* is the unique pair of field and embedding so that the following diagram works out:

In category theory terms, the field of fractions of R is universal with respect to the property of embedding R into a field F.

Where i is the natural embedding of R into its quotient field and f is an injective ring homomorphism into a field E.

Indeed, we can just define $f^*(a/b) = f(a)/f(b) = f(a)f(b)^{-1}$.

Examples of Quotient Fields When we pick the integral domain $\mathbb{Z}$, we obtain the quotient field $\mathbb{Q}$, as expected. When we pick the ring of polynomials (soon to be defined rigorously), we get the rational functions as the quotient field. Taking the quotient field of a quotient field returns itself.

0.4 The Chinese Remainder Theorem

The goal is to eventually look at direct product decompositions of groups and rings. To that end, we introduce the Chinese Remainder Theorem.

Definition: The **direct product** of a finite list of commutative rings is defined as their product as abelian groups, with multiplication defined componentwise.

We also need the following definition:

Definition: Two ideals A, B in a commutative ring R are comaximal if $A + B = R$.

For example, in the ring of integers, the principal ideals generated by any two two coprime integers are co-maximal, and this is the prototypical example. Finally, we are ready to state the theorem:

Theorem (Chinese Remainder Theorem) Let A_i be a finite set of ideals in a commutative ring R. Then the map $\phi : R \to R/A_1 \times R/A_2 \times ... \times R/A_k$ defined by $r \mapsto (r + A_1, r + A_2, ..., r + A_k)$ is a ring homomorphism with kernel $\cap_{i=1}^{k} A_i$.

Furthermore, if the ideals A_i are pairwise comaximal, then the map ϕ is surjective and $\cap_{i=1}^{k} A_i = \Pi_{i=1}^{k} A_i$.

Proof We will prove the case for $k = 2$, and the rest of the proof follows by induction. First, we note that ϕ is of course a ring homomorphism since each natural projection map is a homomorphism, and the kernel is evident.

Say we are working with only two ideals A, B which are comaximal. Since $A + B = R$, we can find $x + y = 1$ with $x \in A, y \in B$. Thus, $x = 1 - y$ mod $B = 1$ mod B, and similarly $y = 1$ mod A.

So our map has $\phi(x) = (0, 1)$, and $\phi(y) = (1, 0)$. Now, we know the map is surjective, since if we pick arbitrary $a, b \in R$, then $\phi(ax + by) = (a + A, b + B)$.

We already knew that $AB \subset A \cap B$, since ideals are closed under left multiplication by any element in R. Furthermore, if $c \in A \cap B$, then $c = cx + cy \in AB$, so indeed $A \cap B \subset AB$ and the two are equal.

We could continue this argument inductively by setting $A = A_1$ and $B = A_2...A_k$ (which, as we saw earlier, is an ideal).

In particular, this tells us that $\frac{\mathbb{Z}}{mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ if m, n are relatively prime. We can therefore find a unique solution to a particular class of Diophantine equations.

As a corollary, considering the multiplicative groups of $\frac{\mathbb{Z}}{n\mathbb{Z}}$, we can prove that the totient of an integer is exactly the product of the totients of its prime power factors.