Rings and Modules

Edmonton, Alberta, Canada

Jacob Denson

$\boxed{\mathcal{JD}}$
2015

Table Of Contents

CHAPTER 1

Basic Definitions

Rings are introverted mathematical creatures, perhaps due to their youthful nature (defined only in the 20s). They may seem to have a cold character to begin with, but after a bit of introduction and a time or two, they'll warm up to you. Lets get to know them a little:

Definition 1. A ring is a set X upon which an additive and multiplicative operation is defined. The additive operation gives the set an abelian group structure, while the multiplicative operation has a monoid structure (not-necessarily commutative). The additive and multiplicative structures play nice with each other, thanks to 'the distributive law': for any three elements a, b, and c in X,

$$a(b+c) = ab+ac \qquad (b+c)a = ba+ca$$

Note that one equation does not imply the other due to the fact that the multiplicative operation is in general not abelian.

Now that you know what a ring is, it turns out that you've known quite a few rings for quite a while. Your favourite fields, be they $\mathbf{R}$, $\mathbf{Q}$, or the finite fields, are all rings, and $M_n(\mathbf{F})$ is a ring for any field also, as are polynomials with coefficients in these rings. There are many other examples. Rings naturally arise when we start studying symmetries upon symmetric structures. Matrices are symmetries of vector spaces, which themselves can be seen as shifting symmetries of space. Polynomials are symmetries over a field of numbers, which themselves are also very well behaved symmetries. In fact, though we have axiomatized rings abstractly, we have a concrete representation theorem for them. Every ring is a set of symmetries over some abelian group. To attempt to find something like this, let us consider the set of endomorphisms on an abelian group. If we surplant a ring structure on this set of morphisms by defining $f+g$ as $(f+g)(x) = f(x)+g(x)$, and defining multiplication as composition. In fact, we actually have a representation theorem of rings just like the representations of a group as a symmetry.

Theorem 1.1. All rings naturally arise as endomorphism of an abelian group.

Proof. Let R be a ring, and consider the set A of group homomorphisms on the abelian additive structure of R. We will show that R can be embedded in A in a natural way. Consider the map $\varphi : R \to R^R$ defined by $\varphi(y) = f_y$, where $f_y : R \to R$ is a map defined by $x \mapsto yx$. Since the distributive law in R holds, we have that

$$f_y(x+z) = y(x+z)yx + yz = f_y(x) + f_y(z)$$

which means exactly that f_y is a morphism, so that $\varphi(R)$ is contained in A. What's more, φ is a morphism, since

$$f_{y+z}(x) = (y+z)x = yx + zx = (f_y + f_z)(x)$$

$$f_{yz}(x) = (yz)x = y(zx) = (f_y \circ f_z)(x)$$

$$f_1 = \mathbf{1} \qquad\qquad f_0(x) = 0x = 0$$

And what's more, φ is injective, since if $f_x = f_y$, then

$$f_x(1) = x = f_y(1) = y$$

Thus A naturally contains R. □

This theorem doesn't really give you a nice answer to what a ring 'really is', unlike Cayley's argument. Alas, most general theories in mathematics do not have natural correspondences with a single object of study, unlike the niceities of group theory. Nonetheless, just like Cayley's theorem gives us group actions on sets, the study of modules will show how we can apply this idea to modules on abelian groups.

There are many nicknames for a ring. When $1 \neq 0$, and every non-zero element has a multiplicative inverse, we say the algebraic object formed is a division ring, or skew field. Commutative division rings are called fields. Not all division rings need be commutative (look up the quaternions if you don't believe me). The basic idea of quaternions results in the following equations

$$i^2 = j^2 = k^2 = ijk = -1$$

extended to general combinations of i, j and k. Invented by the irishman lord Hamilton, quaternions were one of the first truly abstract structures which had operations placed on them, and therefore have a special place in an algebraist's heart.

The other historic structure which gave rise to modern abstract algebra was considered by George Boole, an english logician, when analysing logic abstractly through boolean equations. In his honour, we call a ring R boolean if $x^2 = x$ for all x (and also because of the rings connection to the equations he studied). Any boolean ring is commutative, since $1 = xyxy$, which implies, by multiplying by

yx on the right $yx = xy$. These are essentially the same as boolean algebras studied in logic.

Subrings are the counterpart of subgroups in ring theory. The most fundamental chain of subrings are

$$\mathbf{Z} < \mathbf{Q} < \mathbf{R} < \mathbf{C}$$

Diagonal matrices in $M_n(\mathbf{F})$ form a subring, as do continuous functions in $\mathrm{Mor}(\mathbf{R}, \mathbf{R})$.

If R is a ring, we can pick and choose the elements that can be paired with a nice inverse (both left and right) to form the multiplicative group of units R^*. We require that elements have both a left and right inverse since it may be true that $ab = e$, but $ba \neq e$. Examples of the groups of a units of a ring include the set $GL_n(\mathbf{F})$ (the units in the ring $M_n(\mathbf{F})$) and, in the set $\mathrm{Mor}(X, \mathbf{R})$, the set of functions that vanish nowhere.

A ring homomorphism from a ring A to a ring B is a function $f : A \to B$ such that

$$f(a+b) = f(a) + f(b) \qquad f(ab) = f(a)f(b)$$
$$f(1) = 1 \qquad f(0) = 0$$

Interestingly, there is a homomorphism from the integers to any ring. They are in some sense the fundamental ring object.

CHAPTER 2

Ideals

The kernel of a ring homomorphism is the kernel of the homomorphism seen as a homomorphism between abelian groups. A ring homomorphism is an isomorphism if and only if the kernel is trivial. Things to notice about any kernel K is that it is a abelian subgroup of the domain of the homomorphism A such that $AK \subset K$ (and hence $AK = K$). More generally, we define any subset of a ring to be a (left) ideal if it satisfies these properties. This is ala the definition of a normal subgroup in group theory.

The ideal of a ring, like the normal subgroup of a group, allows us to form the quotient of the algebraic structure of the ring. Given a abelian subgroup I of a ring R, we may form the quotient subgroup R/I. If I is an ideal, we may define $(a+I)(b+I) = ab+I$. This gives us a ring structure on the quotient group. Just like groups, we obtain important isomorphism theorems.

Theorem 2.1. If $f : A \to B$ is a surjective ring homomorphism, then $A/\ker f \cong B$.

Theorem 2.2. If $f : A \to B$ is a surjective homomorphism, there is a one-to-one correspondence with ideals of B and ideals of A that contain the kernel of f.

A ring itself, and its trivial subring (0), are always ideals in some ring, and are called trivial. In a field, these are the only ideals (from which we can deduce that a non-trivial field homomorphism is injective). Other examples in a ring R are Ra, where a is a ring element. This ideal is called the principal ideal generated by a. If a ring is such that all ideals are of this form, we say the ring is principal. Any ideal can be generated by these ideals in the sense that all ideals are $\bigoplus_{i \in I} Ra_i$, and we say the set of a_i generate this ideal. In particular, if I can be selected as finite, we say the ideal is finitely generated.

Quite a bit of elementary ring theory is an attempt to generalize what makes the integers so nice. The integers are a principal ideal domain, and almost any additional property that can be applied to rings will holds for integers. This is because integers are universal objects in ring theory – they are the initial objects in the category. A ring is entire, or forms an integral domain, if it contains no zero-divisors. That is, if $ab = 0$ for two elements a and b, then $a = 0$ or $b = 0$. In particular, if a principal ring is entire it is called a principal ideal domain. This removes some of the nasty properties inherent in the general definition of rings.

An element x is nilpotent if $x^n = 0$ for some integer $n > 0$. If $1 \neq 0$ in a ring, then a nilpotent element is not invertible. The set of all nilpotent elements in a **commutative** ring R is an ideal, denoted $\sqrt{R}$ and called the nilradical of the ring. The additive closure of $\sqrt{R}$ follows from the binomial theorem. If $x^n = 0$ and $y^m = 0$, then

$$(x-y)^{nm} = \sum_{k=0}^{nm} \binom{n+m}{k} x^{n+m-k} y^k (-1)^k$$

each element in the sum has some nilpotent power in. Hence $(x-y)^{nm} = 0$.

Given any ring R, there is a unique homomorphism from $\mathbf{Z}$ to R. The kernel of this homomorphism is an ideal of $\mathbf{Z}$, and since $\mathbf{Z}$ is a principal ideal domain, can be denoted $n\mathbf{Z}$ for some integer n. n is the characteristic of the ring R.

The property of idealness is preserved by many set theoretic operations. For instance, if A is a set of ideals, then so is

$$\bigcap A$$

and provided A forms a chain linearly ordered by inclusion, so is

$$\bigcup A$$

Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$, we define an operation of multiplication

$$\mathfrak{a}\mathfrak{b} = \{\sum a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

This is the smallest ideal containing all $a_i b_i$. $\mathfrak{a} + \mathfrak{b}$ is similarily an ideal. More generally, so is $\bigoplus \mathfrak{a}_i$ for any so specified family of ideals. Given any subset of a ring, we can generate a smallest ideal containing it by the same mathematical trick used in all disciplines of mathematics - just take the intersection of all possible candidates.

As an example of this process, consider ideals in $\mathbf{Z}$. Since $\mathbf{Z}$ is a principal ideal domain, we need only consider products of the form

$$\prod_{i \in I} p_i \mathbf{Z}$$

which is generated by all integers that can be written

$$\prod_{i \in I} s_i p_i$$

with s_i in $\mathbf{Z}$. Since all of the products can be written $\prod s_i \prod p_i$, we get that $\prod p_i\mathbf{Z} \subset \mathbf{Z}(\prod p_i)$. Since we may take all $s_i = 1$, we obtain that $\prod \mathbf{Z}p_i = \mathbf{Z}\prod p_i$.

A prime number is a number p such that if p divides ab, p divides a or p divides b. Equivalently, it is a number such that if $p = ab$, then a or b are ± 1. A prime ideal is an ideal in a ring which is not the entire, ring, and such that if the ideal contains ab, it also contains a and b. It is a small exercise to verify that a ring is entire if and only if (0) is a prime ideal. If a ring is an integral domain, the characteristic of the ring is 0 or a prime number.

An ideal is maximal if it does not contain all ring elements, and there is no ideal containing it but the entire ring, and the ideal itself is not the entire ring. Using Zorn's lemma in the classical manner, one may verify that any ideal is contained in some maximal ideal. Maximal ideals in some sense take the nastiness out of a ring.

Theorem 2.3. *I is a maximal ideal of a ring R if and only if R/I is a field.*

Proof. We will verify that R/I is a field, and leave the converse to the reader. In R/I, $1 \neq 0$, since $1 \notin I$. Consider $x + I$, where $x \notin I$. Then $I + Rx$ is an ideal strictly bigger than I, so that $I + Rx = R$. Thus there is $y \in R$, $z \in I$ such that $z + yx = 1$. But then $yx + I = 1 + I$, so $y + I = (x + I)^{-1}$. □

In the case of the ring $\mathbf{Z}$, the maximal ideals are $p\mathbf{Z}$, where p is a prime number. We already know that $\mathbf{Z}/p\mathbf{Z}$ is a field.

We can also use Zorn's lemma to generalize the nilradical of a commutative ring to noncommutative cases. We define the Jacobson radical $J(R)$ of a (not necessarily commutative) ring R to be the intersection of all prime ideals in the ring; it is the smallest prime radical. In the commutative case, $J(R) = \sqrt{R}$.

Theorem 2.4. *In a commmutative ring, the Jacobson radical is equal to the nilradical of the ring.*

Proof. First we must show that every prime ideal contains every nilpotent element. If $x^n = 0$, then, since every prime ideal I contains 0, $x^n \in I$. By definition of the prime ideal, $x \in I$. Conversely, suppose $x \notin \sqrt{R}$. Consider the set $S = \{x^n : n \in \mathbf{N}\}$. Let L be the set of all (not necessarily prime) ideals in R disjoint from S. L is not empty, since $(0) \in L$, and L is inductively ordered, so we may consider some upper bound P. Given any $a, b \notin P$, $P + Ra$ and $P + Rb$ are strictly bigger than P, and thus there is p_1, r_1 and p_2, r_2 such that $p_1 + r_1 a = x^n$ and $p_2 + r_2 b = x^m$. But then

$$x^{m+n} \in (P + Ra)(P + Rb) = P + P(Ra) + P(Rb) + Rab = P + Rab$$

And therefore $ab \notin P$. Thus P is prime, and does not contain x, so that $J(R)$ does not contain x. □

CHAPTER 3

Polynomials

Let R be a ring. By $R[x]$, we mean the set of all finite formal linear combinations $\sum_{k=0}^{\infty} r_k x^k$, where $r_k = 0$ for all but finitely many k. We define addition and multiplication by

$$\left(\sum_{k=0}^{\infty} r_k x^k\right) + \left(\sum_{k=0}^{\infty} l_k x^k\right) = \sum_{k=0}^{\infty} (r_k + l_k) x^k$$

$$\left(\sum_{k=0}^{\infty} r_k x^k\right)\left(\sum_{k=0}^{\infty} l_k x^k\right) = \sum_{k=0}^{\infty} \left[\sum_{i+j=k} (r_i + l_j)\right] x^k$$

$R[x]$ is a ring, and is commutative if R is.

If $f \in R[x]$, we define the degree of f to be the maximum $r_k \neq 0$ in the coefficients of f. Polynomials of degree 0 are called constants, linear polynomials are of degree 1, quadratic are degree 2, etc. By custom, if $f = 0$, we define $\deg(f) = -\infty$.

Theorem 3.1. If R is entire, then $\deg(fg) = \deg(f) + \deg(g)$. In general, $\deg(fg) \leq \deg(f) + \deg(g)$.

Proof. Let $f = \sum_{k=0}^{n} r_k x^k$ and $g = \sum_{k=0}^{m} l_k x^k$, then if $fg = \sum q_k x^k$ we have $q_k = 0$ for all $k > n + m$, and $q_{n+m} = r_n l_m \neq 0$, since r_n and $l_m \neq 0$. □

Corollary 3.2. If R is entire, then $R[x]$ is entire.

Theorem 3.3 (Euclidean Division). With the deg function, if k is a field, $k[x]$ is a euclidean domain. That is, for any f, and nonzero g, we may write

$$f = gh + r$$

where h and r are polynomials, and $\deg(r) < \deg(g)$, or $\deg(r) = 0$.

Proof. Let $f = \sum a_k r_k$. We prove this by induction (our proof is very similar to the case of showing the integers are a euclidean domain). If $\deg(g) = 0$, then $g = r_k$, and $f = g(f/r_k)$. Here r is of degree $-\infty$. Now suppose $\deg(g) = n$, and we have proved the theorem for all polynomials of smaller degree. Let the highest coefficient of f be a_k. □

CHAPTER 4

Modules

In the primordial goo from which all groups descend lies the symmetric group $Sym(A)$. Regardless of the complex nature the evolutionary process has granted a specific group, we can still relate it back to its common ancestor by Cayley's theorem. By studying the actions of a group that relate it back to its first ancestor, we obtain many useful structure theorems related to the group itself. The counterpart to a group action on a G-set is a ring action on an R-module, a theory which we will develop in this chapter. The following lemma gives some intuition behind the theory undertaken

Lemma 4.1. Every ring can be embedded in a set of endomorphisms of an abelian group. (note the similarity to Cayley's theorem)

Proof. Let R be a ring. Let us denote by R_G the same object, but viewed solely as an abelian group (the ring's additive structure). For each $r \in R$, consider the group endomorphism $f_r : R_G \to R_G$ defined by $a \mapsto ra$. The distributive law tells us that R_G is an endomorphism. That is,

$$f_r(a+b) = r(a+b) = ra + rb = f_r(a) + f_r(b)$$

Now let us show that the map $\varphi : r \mapsto f_r$ embeds R in $End(R_G)$. The distributive law for the left side tells us that

$$f_{a+b}(x) = (a+b)x = ax + bx = f_a(x) + f_b(x)$$
$$f_1(x) = 1x = x$$
$$f_{ab}(x) = (ab)(x) = a(bx) = f_a(f_b(x))$$

These equations tell us that φ is a ring homomorphism. Now if $f_a = f_b$, then $f_a(1) = f_b(1)$, so that $a = b$. Thus φ is injective. □

The axioms for a ring have been perfectly aligned with the statement for this theorem, as group have for Cayley's theorem.