Ring Theory

Jacob Denson

January 19, 2016

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. A **ring** is a set R upon which an additive and multiplicative operation is defined (with respective identities 0 and 1). The additive structure forms an abelian group, the multiplicative structure a (not-necessarily commutative) monoid structure. The additive and multiplicative structures play nice with each other thanks to the 'distributive law': for any $a, b, c \in R$,

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

Note that one equation does not imply the other due to the fact that the multiplicative operation is in general not abelian. We assume $1 \neq 0$, since if $1 = 0$ the theory is trivial.

You already know many rings. Your favourite number systems, be they $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{Q}$, or $\mathbf{F}_p$, are rings, as are the set of all matrices $M_n(\mathbf{F})$, and polynomials $\mathbf{F}[X]$ over some field. Rings arise naturally when we start studying symmetries of preexisting algebraic 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, every ring can be seen as a set of symmetries over some abelian group.

Example. *Let G be an abelian group, and consider* $\mathrm{End}(G)$*, the set of all homomorphisms from G to itself. We define a ring structure on this set. Let $(f+g)$ be defined pointwise, and let composition $f \circ g$ be the multiplicative structure. The fact that* $\mathrm{End}(G)$ *satisfies the laws of a ring are trivial, with the identity endomorphism behaving as* 1*, and the trivial homomorphism acting as* 0*.*

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

Proof. Let R be a ring, and consider the set $\mathrm{End}(R^+)$ of group homomorphisms on the abelian additive structure of R. We will show that R can be embedded in $\mathrm{End}(R^+)$ 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 $\mathrm{End}(R^+)$. What's more, φ is a ring morphism (which by now, you should be able to provide a definition for), since

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

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

$$f_1 = \mathrm{id}_R \qquad f_0(x) = 0x = 0$$

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

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

Thus $\mathrm{End}(R^+)$ naturally contains R. □

The problem with this proof is that the theorem doesn't really give a 'nice' answer to what a ring really is. Groups are already abstract, so we may not necessarily be able to visualize what a symmetry of an arbitrary abstract object is. Alas, most general theories in mathematics do not have natural correspondences with a single object of study, unlike the niceities

of group theory. This is to be expected, since ring theory arose from many fields of study, like number theory, geometry, and logic. We will just have to accept this theorem as a little tidbit of intuition, and move on. We will return to this idea in the theory of modules, where one studies a ring 'acting' on an abelian group, just like Cayley's theorem gives us group actions on sets.

Definition. The **units** of a ring R are the elements x which possess a multiplicative inverse x^{-1}, a number such that $xx^{-1} = 1 = x^{-1}x$ (both ends of the equation need to be satisfied since ab may not equal ba). We shall denote the set of units by $R^\times$ or $U(R)$. This set always forms a group. though not necessarily a subring. Every non-zero element of a **division ring** (also called a **skew field**) is a unit. Commutative division rings are called **fields**.

Example. *The group of units in $M_n(\mathbf{F})$ is the general linear group $GL_n(\mathbf{F})$.*

Left invertible elements need not be right invertible.

Example. *Consider the set $\mathbf{R}^\mathbf{N}$ of real-valued sequences, which form an abelian group under pointwise addition. Take the set of morphisms on this set. This consists of two maps – the left shift L and the right shift R:*

$$L(x_0, x_1, x_2, \dots) = (x_1, x_2, \dots) \qquad R(x_0, x_1, \dots) = (0, x_0, x_1, \dots)$$

Then $L \circ R = \mathrm{id}_{\mathbf{R}^\mathbf{N}}$, yet $R \circ L(x_0, x_1, \dots) = (0, x_1, \dots)$, and L could never have an inverse, since it is not bijective.

Not all division rings need be commutative.

Example. *Let G be a group, and K a field. The group ring $K[G]$ is the set of all finite sums $\sum k_i g_i$, with $k_i \in K$ and $g_i \in G$, where the additive structure is obvious, and*

$$\left(\sum_i k_i g_i\right)\left(\sum_j k'_j h_i\right) = \sum_{i,j} k_i k'_j g_i h_j$$

The quaternion group is $Q = \{1, i, j, k\}$, where

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

The general quaternions are the group ring $\mathbf{R}[Q]$. *Every non-zero quaternion is invertible, since*

$$\begin{aligned}(a+bi+cj+dk)(a-bi-cj-dk) &= a^2+b^2+c^2+d^2 \\ &= (a-bi-cj-dk)(a+bi+cj+dk)\end{aligned}$$

Quaternions are not commutative, since $ij = k$, $ji = -k$. *Invented by the Irishman, lord Hamilton, quaternions were one of the first truly abstract algebraic structures, and therefore have a special place in an algebraist's heart.*

Example. *George Boole began the modern study of logic by studying truth. He saw that the logical operations of conjunction and disjunction behaved very similarily to the algebraic operations of multiplication and addition. If we consider conjunction as the multiplicative structure in a set of statements, and exclusive disjunction as an additive structure (where two statements are equivalent if they both imply each other), then we obtain a ring, satisfying* $x^2 = x$ *for all statements* x *(where 0 is a statement which is always false, and 1 a statement which is always true). In his honour, we call a ring* **boolean** *if this equation is satisfied. 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.*

As with groups, one may consider subrings of a ring, and homomorphisms between rings. By now, you should be able to figure out the definitions yourself, but for completeness, they are included below.

Definition. A **subring** of a ring is a subset of a ring which also possesses a ring structure. That is, a subring is closed under addition and multiplication.

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 the continuous functions in $\mathrm{Mor}(\mathbf{R}, \mathbf{R})$.

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

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

1.1 Ideals

We wish to establish a quotient structure on rings, to obtain analogies to the isomorphism theorems for groups. Let $\mathfrak{a}$ be a subset of a ring A. In order to obtain a well defined addition operation, we first need $\mathfrak{a}$ to be an additive subgroup of the additive group structure on $\mathfrak{a}$. We also require that the act of multiplication is well defined:

$$(a + \mathfrak{a})(b + \mathfrak{a}) = (ab + \mathfrak{a})$$

So, in terms of sets,

$$\{(a+x)(b+y) = ab + xb + ay + xy : x, y \in \mathfrak{a}\} = \{ab + x : x \in \mathfrak{a}\}$$

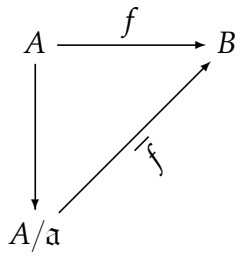
Thus we require $xb + ax' + xx' \in \mathfrak{a}$. Clearly, not only do we need $\mathfrak{a}$ to be closed under multiplication, but also closed under multiplication by any element of A. This is the definition of an ideal.

Definition. A **left ideal** $\mathfrak{a}$ is an additive subgroup of a ring A, with $A\mathfrak{a} = \mathfrak{a}$. A **right ideal** satisfies $\mathfrak{a}A = \mathfrak{a}$. A **double-sided ideal** (shortened to **ideal**) is a left and right ideal, and is the structure we use to form a quotient ring $A/\mathfrak{a}$.

We shall focus mostly on double sided ideals (which are the same as single sided ideals in the commutative case). One sided ideals come into play most importantly when we analyze modules.

The kernel of a ring homomomorphism is a double sided ideal. A ring homomorphism is an isomorphism if and only if the kernel is trivial. Just as in the group-theoretic case, we obtain the first isomorphism theorem.

Theorem 1.2 (First Isomorphism Theorem)**.** *Let $f : A \to B$ be a homomorphism of rings. If $\mathfrak{a}$ is a double-sided ideal contained in the kernel of f, then we have an induced homomorphism $\overline{f} : A/\mathfrak{a} \to B$ satisfying the commutative diagram*



If $\mathfrak{a}$ is the kernel, then the map is injective.

Theorem 1.3 (Second Isomorphism Theorem)**.** *Let $B < A$ be a subring, and $\mathfrak{a}$ an ideal of A. Then $B + \mathfrak{a}$ is a subring, $\mathfrak{a}$ is an ideal in $B + \mathfrak{a}$, $B \cap \mathfrak{a}$ is an ideal in B, and*

$$B/(B \cap \mathfrak{a}) \cong (B + \mathfrak{a})/\mathfrak{a}$$

Theorem 1.4 (Third Isomorphism Theorem)**.** *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 (denoted (1) when viewed as an ideal), and its trivial subring $(0) = \{0\}$, are always ideals, and are called trivial. In a field, these are the only ideals (from which we can deduce that a non-trivial ring homomorphism whose domain is a field 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, and in the commutative case, is denoted (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 $(S) = \bigoplus_{s \in S} Rs$ for some set S, and we say that S generates the ideal. In particular, if S can be selected as a finite set, we say the ideal is finitely generated.

There is one and only one homomorphism from the integers to any ring (a simple proof by induction). They are in some sense the fundamental

ring object. The kernel of such a map is of the form (n), for a unique positive integer n. We call n the **characteristic** of the ring, and $\mathbf{Z}_n$ the **prime ring** contained within the ring. Note that this is the smallest subring.

Quite a bit of elementary ring theory is an attempt to generalize what makes the integers so nice. Integers are universal objects in ring theory – they are the initial objects in the category. Since homomorphisms relate properties of rings, integers should naturally possess nice properties.

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

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

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 1.5. *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 $y + I = (x + I)^{-1}$. $\square$

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 1.6. *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 2

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 2.1. *If R is entire, then* $\deg(fg) = \deg(f) + \deg(g)$. *In general,* $\deg(fg) \leqslant \deg(f) + \deg(g)$.

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 2.2. *If R is entire, then $R[x]$ is entire.*

Theorem 2.3 (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. □

2.1 Commutative Rings

Definition. A factorial ring A is an integral domain such that every a can be written

$$a = \prod_{i=1}^{n} p_i$$

where p_i is irreducible, and if

$$\prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$$

Then $n = m$, and, after a permutation, each p_i differs from q_i by a unit.

Lemma 2.4. *An element $x \in A$ is invertible in $S^{-1}A$ if and only if $(x) \cap S \neq \varnothing$.*

Proof. If $x(m/n) = 1$, $xm = n \in S$. Conversely, if $xm \in S$, then $x(m/xm) = 1$. □

Lemma 2.5. *If p is prime in A, then it is irreducible in $S^{-1}A$, provided it is not a unit.*

Proof. If $p = (m/n)(x/y)$, and it is not a unit, then $nyp = mx$, so that $p \mid mx$. It follows that $p \mid m$ or $p \mid x$. In either case, we divide by p to conclude either m/n or x/y is a unit. □

Lemma 2.6. *Let A be factorial. a/b is irreducible if and only if $a/b = up$, where $u \in U(S^{-1}A)$, and p is irreducible in A and $S^{-1}A$.*

Proof. Let $a = p_1 \dots p_n$, and $b = q_1 \dots q_n$, where p_i and q_i are irreducible in A, then some p_i is irreducible in $S^{-1}A$, and the other combined factors are a unit. But this implies exactly that p_i is irreducible in A, and $(p_i) \cap S = \varnothing$. □

Lemma 2.7. *If y differs from x by a unit, and y is uniquely factorizable, then x is uniquely factorizable.*

Proof. Write $x = yu$, where y is factorizable, $y = p_1 \dots p_n$, then $x = up_1 \dots p_n$. Now suppose that x can be factorized in two ways

$$x = p_1 \dots p_n = q_1 \dots q_m$$

Then,

$$ux = (up_1)p_2 \dots p_n = p_1' \dots p_n' = (uq_1)q_2 \dots q_m = q_1' \dots q_n'$$

so, up to a permutation, $p_i' = u_i q_{\pi(i)}'$. But one verifies, by taking the vary cases, that this implies that $p_i = v_i q_{\pi(i)}$, where v_i is a unit. □

Theorem 2.8. *If A is factorial, and S is a multiplicative set with $0 \notin S$, then $S^{-1}A$ is factorial.*

Proof. Let a/b be given. We need only verify that a/b differs from a uniquely factorizable element by a unit. a differs from a/b by a unit. Write $a = p_1 \dots p_n$, where p_i is irreducible in A. We know that each p_i is either still irreducible, or a unit, so without loss of generality we may as well assume all p_i are irreducible in $S^{-1}A$. Suppose

$$p_1 \dots p_n = (u_1 q_1) \dots (u_m q_m) = (u_1 \dots u_m q_1) q_2 \dots q_m$$

Let $u_1 \dots u_m = x/y$. If $u_1 \dots u_m$ can be written as the quotient of two units in A, then we are done, for then the p_i and q_i differ by units in A, and thus the p_i differs from $u_i q_i$ by a unit. We show this is the only case that could happen, since we assume the p_i are irreducible in $S^{-1}A$.

If y is not a unit in A, write $y = y_1 \dots y_k$. If x is a unit in A, then when we apply unique factorization in A, we see y_1 differs from some p_i by a unit in A. But y_1 is a unit in $S^{-1}A$, so that p_i is a unit in $S^{-1}A$. If x is not a unit, then we may consider $x = x_1 \dots x_l$, and may assume no x_i and y_j differ by a unit (by cancelling like terms), so that when we apply unique factorization, y_1 is mapped to p_i again, contradicting the irreducibility of

p_i. Thus y must be a unit in A, and when we expand x as we have already done, and write

$$(p_1/y)\dots p_n = x_1 \dots x_l q_1 \dots q_m$$

But then some x_i differs from a p_j by a unit in A, hence p_j is a unit in $S^{-1}A$. □

Chapter 3

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 3.1. *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.