0.1 Rings

Algebra is the study of mathematical *structures* and the possible, structure respecting *maps* that can be constructed between them. One of the most important of the structures in modern algebra is called *the ring*. It was defined in the late 1800's by Kummer while working on the problem of unique factorization. The name comes from his early examples, which were number systems including elements, such as the imaginary quantity i, which when taken to successive powers, eventually circle around onto themselves.

A set of elements is a ring if there are two functions on the set, called addition and multiplication, which abide by a long list of properties.

1. Both addition and multiplication must be associative, binary operations.

2. Addition is an abelian group. That is, for every element a in the group there is a unique inverse $-a$, and there is a unique *zero element* 0 for which $a+0 = 0+a = a$ for any a in the group. Addition is also required to be commutative, $a + b = b + a$ for any a and b in the group.

3. Multiplication left and right distributes over addition: $a(b+c) = ab+ac$ and $(b + c)a = ba + ca$, any a, b and c.

4. Typically by ring one means *a ring with unit*. That is, there is a unique *unit element*, aptly denoted 1, for which $a1 = 1a = a$ for any element a.

A *commutative ring* is a ring in which multiplication is commutative. The most common rings in everyday life are commutative with unit.

The definition of an abelian group might be better understood by the alternative definition. A group (abelian or not) is a set of elements for which the equations $a + x = b$ and $x + a = b$ always have a unique solution for x given any a and b. One sees here the need for the definition of a group — it corresponds to the need to solve simple equations. If one writes $a + x = a$, then it implies the existence of a zero element. And if one writes $a + x = 0$, it implies for every a the existence of a unique inverse.

Examples:

- The integers $\{\ldots,-1,0,1,2,\ldots\}$ with the standard addition and multiplication operations form a ring.

- The integers modulo some number $\{0,1,2,\ldots N-1\}$ with modular arithmetic, form a ring.

- Polynomials with coefficients in a ring, form a ring. For instance, polynomials in x and y with integer coefficients, denoted $\mathbf{Z}[x,y]$. As example elements we can give $1, 5x+2$ or $7x^3y+9xy+2x+1$.

0.2 Map of rings

As important and structures are the maps between structures. In this way we can say that two obects are the same or delineate how they differ. Well chosen maps can make problems easy to solve by highlighting the most important structural imperatives. Suppose R and R' are two rings. A map of these rings can be more than a passive pairing of items in R with items in R'. It might *respect* or *preserve* the ring structures. Often a map between two rings is tacitly assumed to preserve the ring structure, or one can be explicit by saying that is is a *map of rings.*

Concentrating our attention on rings, a map $f: R \to R'$ preserves addition if for any r_1 and r_2 of R,

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

What this is saying that the same element of R' results either if one first adds then maps or first maps then adds. Another way of looking at it is to see "phantom" hands adding the "shadows" of r_1 and r_2 in R' as you add them in R. Your result and the phantom's result would agree.

When an correspondence, or *map*, preserves an operation, we can expect it to preserve properties which are a necessary result of the operation. For instance, it the above correspondence preserves addition, and r_1 happens to be the inverse of r_2, then it must be that ${r_1}'$ is the inverse of ${r_2}'$. We leave a proof of this to the reader.

A map $f: R \to R'$ between two rings R and R' is a *map of rings* if it preserves addition, multiplication and the unit element. That is,

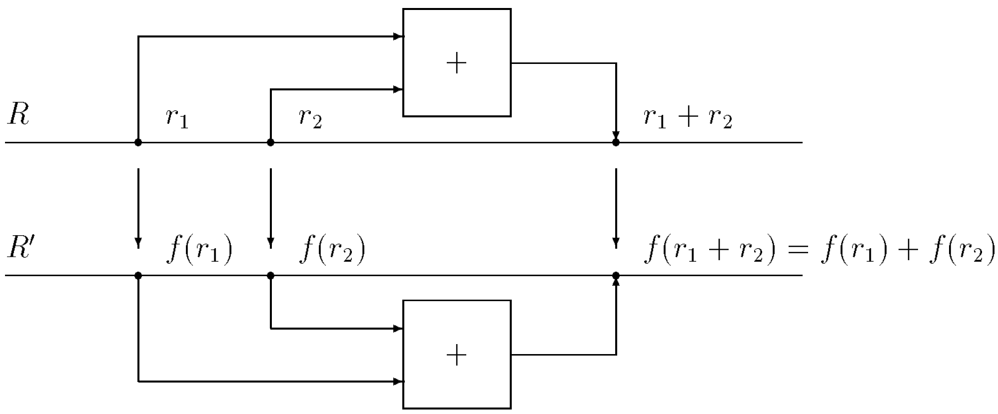

Figure 0.1: A map of rings preserves addition.

1. For any $x, y \in R$, $f(x + y) = f(x) + f(y)$. It follows logically that $f(0) = 0'$, where 0 and $0'$ are the zero elements of R and R', respectively, and that $f(-x) = -f(x)$, for any x.

2. For any $x, y \in R$, $f(xy) = f(x)f(y)$.

3. If 1 and $1'$ are the unit elements in R and R', respectively, $f(1) = 1'$.

In the theory of rings without unit, the third condition would not be included.

0.3 Ideals and Quotient Rings

The rings Kummer worked with often had difficiencies in their structure. Namely, the principle of unique factorization into irreducibles failed. He perceived that the principle could be recovered if elements were introduced into to ring as new factors for many elements. He considered these elements *ideal* since they existed in order to fulfill the ideal of unique factorization. It was later discovered that such elements needn't be created from nothing, they could be found by taking subsets of existing elements. And it was soon discovered that these subsets, called *ideals*, were the basic building blocks of any map of rings.

Given a ring R, an ideal I in R is a non-empty subset of R which is closed by addition and additive inverses and by multiplication by any element of R. That is,

1. The set I is closed by addition: if i and i' is in I, then $i + i'$ is in I.

2. The set I is closed by additive inverses: if i is in I, then $-i$ is in I.

3. The set I is closed by multiplication by any element of R: if i is in I and r is in R, then ir and ri must be in I.

Given an ideal I in R, and an element r of R, the *translate of I by r* is the set:

$$r + I = \{\, r + i \,|\, i \in I \,\}.$$

The collection of translates of an ideal of a ring can itself be given the structure of a ring. It is called the *quotient ring* of the ring by the ideal. The current goal is to describe more fully the creation of the quotient ring.

Theorem 1 *Given I an ideal of R and r_1 and r_2 elements of R, if $r_1 - r_2 \in I$ then $r_1 + I = r_2 + I$, else these two translates have no elements in common.*

PROOF: If $r_1 - r_2 \in I$, then let this difference be i. So $r_1 = r_2 + i$ and r_1 is in $r_2 + I$ as well as in $r_1 + I$. Hence the there is a common element. Conversly, if $r_1 + I$ and $r_2 + I$ share any element in common, then there is an $i \in I$ such that $r_1 = r_2 + i$, which implies that $r_1 - r_2 \in I$. We have shown that the two translates intersect if and only if the difference of the translations is in I.

We go on to show that if the translate intersect, they are identical. Once again, let $r_1 = r_2 + i$ with $i \in I$, by supposition, and for any $r_1 + i'$ in $r_1 + I$, we set let $i'' = i + i'$. Then $r_1 + i'$ is also in $r_2 + I$, because $r_2 + i''$ is in $r_2 + I$ and $r_2 + i'' = r_2 + i + i' = r_1 + i'$. We also show likewise that any $r_2 + i$ in $r_2 + I$ is in $r_1 + I$. So these sets are exactly the same. □

We can define addition and multiplication of translates of I so that the set of all translates becomes a ring, called the quotient ring of R modulo I, R/I. Consider the map $\phi : R \to R/I$ which takes $r \in R$ to the translate $r + I$. We define addition and multiplication in R/I so that ϕ is a map of rings. Consider first addition. For ϕ to respect addition, then for any r_1 and r_2 in R,

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2).$$

Hence adding r_1+I and r_2+I should result in $(r_1+r_2)+I$. We can make this the definition of addition in R/I provided all elements of the quotient ring have at least on representation as $r+I$ for some r in R, and if an element of the quotient ring can be represented in two ways, $r_1+I=r_2+I$ for r_1 and r_2 two different elements of R, either representation can be used to determine the result of the addition.

The definition for multiplication is similar. The equation,

$$\phi(r_1 r_2)=\phi(r_1)\phi(r_2)$$

must hold for any r_1 and r_2 in R, so we define,

$$(r_1+I)(r_2+I)=(r_1 r_2)+I.$$

Again, we have the burden of showing that translations equivalent to r_1+I and r_2+I multiply to an translation equivalent to $r_1 r_2+I$.

Theorem 2 *With addition and multiplication as defined, the collection of translations of the ideal I form a ring.*

Proof: We first show that addition and multiplication are defined consistantly, That is, different choices for the representation of a translation don't matter.

Suppose $r_1+I=r_1'+I$ and $r_2+I=r_2'+I$. Then both r_1-r_1' and r_2-r_2' are in I, and so is

$$(r_1-r_1')+(r_2-r_2')=(r_1+r_2)-(r_1'+r_2').$$

Thus $(r_1+r_2)+I=(r_1'+r_2')+I$. This shows that any representation of a translation gives the same result for addition as defined.

If $r_2+I=r_2'+I$ then $r_2-r_2'\in I$, and by the rules of an ideal,

$$r_1(r_2-r_2')=r_1r_2-r_1r_2'\in I,$$

for any $r_1\in R$. Likewise, if $r_1+I=r_1'+I$, then $r_1-r_1'\in I$, and by the rules of an ideal,

$$(r_1-r_1')r_2'=r_1r_2'-r_1'r_2'\in I,$$

for any $r_2'\in R$. The sum of two elements in an ideal rests inside the ideal, so,

$$(r_1r_2-r_1r_2')+(r_1r_2'-r_1'r_2')=r_1r_2-r_1'r_2'\in I.$$

Therefore $r_1 r_2 + I = r_1' r_2' + I$, as was to be shown.

Now that addition and multiplication are defined, we must show that they fulfil the properties of a ring. All the properties enjoyed by R are passed on to R/I, since we can compute in R/I with representatives taken from R. This shows that R being commutative with unit implies that R/I will also be commutative with unit. □

0.4 Applications

We can now see that the integers mod n, for any integer n, is also understood as $\mathbf{Z}/n\mathbf{Z}$. That is, the integers modulo the ideal of all multiples of n.

0.4.1 Ideals in the ring of integers

In the ring of integers $\mathbf{Z}$ there is one ideal for every integer m in $\mathbf{Z}$ and it is the set of all multiples of m,

$$m\mathbf{Z} = \{\, mi \mid i \in \mathbf{Z} \,\}.$$

Unless m is 1 or -1, the ideal $m\mathbf{Z}$ does not include all integers. We can "translate" the ideal by some integer k,

$$k + m\mathbf{Z} = \{\, k + i \mid i \in m\mathbf{Z} \,\}.$$

Try to imagine what these translates look like on the number line. You have an infinitely long ruler with inches marked off in the positive and negative directions from some arbitrary zero point. The ideal $m\mathbf{Z}$ is the set taking every m-th mark, starting from zero. Keeping this configuration rigid but moving it entirely left or right, you have a picture of the different translates of the ideal.

Given any integer i, it is contained in the translate $i + m\mathbf{Z}$. If one were to take i modulo m in the fashion of our childhood, (where r is equivalent to i mod m, for the r safisfying,

$$0 \leq r < m \text{ and } i = mq + r \quad)$$

then,

$$i + m\mathbf{Z} = r + m\mathbf{Z},$$

where by "equal" we mean that they are exactly the same sets. This is the foundation of another way of looking at the integers modulo m. We can either say that i modulo m is the remainder when i is divided by m, or it is the translate of the ideal $m\mathbf{Z}$ in which i lies.

Addition modulo m also has a reinterpretation as translations of the ideal $m\mathbf{Z}$. The sum of i and j modulo m is the translate $(i+j)+m\mathbf{Z}$. In fact, if i' is any integer in $i+m\mathbf{Z}$, and j' is any integer in $j+m\mathbf{Z}$,

$$(i'+j')+m\mathbf{Z}=(i+j)+m\mathbf{Z}.$$

In the children's approach to modular arithmetic, we might say this in the form:

$$(i \pmod m)+(j \pmod m) \pmod m=(i+j) \pmod m.$$

That is, it doesn't matter when or how often we decide to go modulo m, the result will end up the same. The same is true of multiplication. The product of i and j modulo m is the translate $i'j'+m\mathbf{Z}$ where i' is any integer in $i+m\mathbf{Z}$ and j' is any integer in $j+m\mathbf{Z}$.

0.4.2 Gaussian Integers

Another informative example is the ring of *Gaussian integers.* All of us are familiar with i, the imaginary quantity whose sqaure is minus one. In a similar way that the complex numbers are the reals with the adjunction of i, the Gaussian integers are the integers with the adjunction of i.

Each Gaussian integer can be written as.

$$a+b\,i, \quad a,b\in\mathbf{Z}.$$

To calculate with Guassian integers, we follow the rules,

$$(a_1+b_1\,i)+(a_2+b_2\,i)=(a_1+a_2)+(b_1+b_2)\,i$$

and,

$$(a_1+b_1\,i)(a_2+b_2\,i)=(a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)\,i.$$

We demonstrate the theory of ideals can be used to "construct" the Gaussian integers as a quotient ring of the ring of polynomials with integer coefficients.

Starting from $\mathbf{Z}[x]$, the ring of polynomials in x with integers coefficients, we "force" x to behave as does i. That is, we proclaim that $x^2 + 1 = 0$. Hence every polynomial in the ideal,

$$\mathcal{I} = (x^2 + 1)\,\mathbf{Z}[x],$$

becomes zero. We therefore look at the quotient ring $\mathbf{Z}[x]/\mathcal{I}$ and show that this is exactly the same as the Gaussian integers.

The formal method of doing this might at first make one's head spin, but it is less awesome than it first appears. We define a map ϕ from $\mathbf{Z}[x]/\mathcal{I}$ to the Gaussian integers. We then demonstrate that this map sets up a perfect correspondence between the elements and operations in $\mathbf{Z}[x]/\mathcal{I}$ and the elements and operations of Gaussian integers. That is, the two rings have completely parallel structures, and this is mathematically sufficient to claim that the rings are the same.

Here is the map. Given any element of the quotient ring $\mathbf{Z}[x]/\mathcal{I}$, take any polynomial f in the residue class and consider its remainder when divided by $x^2 + 1$,

$$f = q(x^2 + 1) + r,$$

where r will be a polynomial of the form $bx + a$. Then $\phi(f) = a + b\,i$. Any other f' from the same residue class will give the same result, since $f' - f$ is a multiple of $x^2 + 1$.

We claim that ϕ is a map of rings.

$$\begin{aligned}
\phi(f+g) &= \phi(q_f(x^2+1) + r_f + q_g(x^2+1) + r_g) \\
&= \phi((q_f + q_g)(x^2+1) + r_f + r_g) \\
&= r_f + r_g = \phi(f) + \phi(g).
\end{aligned}$$

The computation for multiplication is more involved:

$$\begin{aligned}
\phi(fg) &= \phi((q_f(x^2+1) + r_f)(q_g(x^2+1) + r_g)) \\
&= \phi((q_f q_g(x^2+1) + q_f r_g + q_g r_f)(x^2+1) + r_f r_g),
\end{aligned}$$

but,

$$\begin{aligned}
r_f r + g &= a_f a_g + (a_f b_g + a_g b_f)x + b_f b_g x^2 \\
&= a_f a_g - b_f b_g + (a_f b_g + a_g b_f)x + b_f b_g(x^2+1),
\end{aligned}$$

setting

$$q = q_f q_g(x^2+1) + q_f r_g + q_g r_f + b_f b_g,$$

we have.

$$\begin{aligned}
\phi(fg) &= \phi(q(x^2+1) + a_f a_g - b_f b_g + (a_f b_g + a_g b_f)x) \\
&= a_f a_g - b_f b_g + (a_f b_g + a_g b_f)\, i \\
&= (a_f + b_f\, i)(a_g + b_g\, i) = \phi(f)\phi(g).
\end{aligned}$$

0.5 The Lattice Theory of Ideals

Having gained our attention, ideals can be investigated as mathematical entities onto themselves. A structure results from the possibility of adding and intersecting ideals. Let A and B be two ideals of a ring R. Then the set of all sums,

$$\{\, a + b \,|\, a \in A,\ b \in B \,\},$$

is also an ideal which we can denote $A + B$. It is easy enough to show that it is an ideal of R and that it is the smallest possible ideal of R containing both A and B.œ The set-theoretic intersection of A and B,

$$\{\, c \,|\, c \in A \text{ and } c \in B \,\},$$

is also an ideal, denoted $A \cap B$, and it is almost axiomatic that is the largest ideal which is contained in both A and B. Finally, there is an absolutely smallest ideal in an ring containing only 0, and a largest, containing everything.

The algebraic structure we wish to place on ideals is that of a *lattice.* In the essential, we have a set of ideals with two operations, the sum and the intersection, such that,

1. Given any two ideals A and B, there exists sum and intersections of them.

2. There is a smallest and a largest ideal, respectively denoted 0 and 1.

3. Both addition and intersection are associative, commutative and idempotent operations. That is,

(a) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$,

(b) $A \cdot B = B \cdot A$,

(c) $A \cdot A = A$,

respectively, where A, B and C are any ideals and $\cdot$ can be either intersection or addition.

4. The *absorption identies* hold:

   (a) $A = A \cap (A + B)$,

   (b) $A = A + (A \cap B)$,

   for any ideals A and B.

In addition, a weakened for of *distributivity* holds,

$$(A \cap B) + (A \cap C) = A \cap (B + (A \cap C)).$$

Haven shown these facts, we have proven that ideals form a *modular lattice* under the operations of addition and intersection.

In the language of Universal Algebra, the role addition plays in this lattice is generally referred to as the *join*, and intersection as the *meet* and are respectively denoted $\vee$ and $\wedge$. We shall continue to use $+$ and $\cap$ for emphasis on lattices of ideals.

In this generality it is also noted that joins and meets can be reconstructed from the relative sizes of the elements. With respect to ideals, the larger of two ideals is the one which contains the other — if neither of the ideals contains the other they are said to be *incomparable* in size. Given this notion, the join or addition of two ideals is always the smallest ideal which contains them both, and the intersection is the largest ideal contained in both.

A lattice can be visualized by its *Hasse Diagram* in which the elements are drawn as points in an arrangement in which height and connecting lines indicate the relative sizes of the elements. For instance, a lattice containing three elements in size order,

$$x \leq y \leq z,$$

would be drawn,

$$\begin{tikzcd} x \arrow[d, dash] \\ y \arrow[d, dash] \\ z \end{tikzcd} .$$

It will be usefull to know that in a distributive lattice the following diagram can not appear embedded in the lattice's Hasse diagram,

$$\begin{tikzcd} & x \arrow[dl] \arrow[ddr] & \\ a \arrow[d] & & \\ c \arrow[dr] & & b \arrow[dl] \\ & y & \end{tikzcd}$$

Which is to say compactly in a picture that in the lattice there are not five elements x, y, a, b and c such that,

1. The element x is larger than any other and y is smaller than any other.

2. The elements a and c are comparable and a is the larger.

3. The element b is incomparable with both a and c.

4. The join of b and either a or c is x and the meet of b with either a or c is y.

In fact, the absence of this diagram embedded in a Hasse diagram is both necessary and sufficient for the lattice to be modular.

In passing the a ring homomorphism, one can inquire what happens to each ideal in the source ring. More precisely, one can take an ideal in the sources, map is elementwise to the target then look at the preimage of this set. The result would be $A \vee K$ where K is the kernel of the map and A is the original ideal. It is a closure operation since this makes ideals grow,

$$A \vee K \geq A,$$

and once done the result is fixed,

$$(A \vee K) \vee K = A \vee (K \vee K) = A \vee K.$$

Another way of looking at this is starting from the lattice of ideals and a certain ideal K in the lattice, one asks what does it look like the lattice of the ring modulo K. It looks like the restriction on the lattice of all things larger than K, where a certain maps takes any A in the lattice to $A \vee K$, which is the smallest ideal larger than K which is also larger than A.

Lattices are further classified by additional algebraic laws among joins and meets. Most important is the *distributive lattice* for which,

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

and,

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Less easily appreciated is the *modular lattice*. Among the distributive lattices are those for which each element has a complement. Sets are complemented distributive lattices. The complement of an element a is the unique element b such that $a \wedge b = 0$ and $a \vee b = 1$.

Implication can also be understood as a lattice operation. In the case that a lattice is complimented, it should be that,

$$a \Rightarrow b = \not a \vee b.$$

However in non-complimented lattices implication is defined as,

$$a \Rightarrow b = \max\{\, x \mid x \wedge a \leq b \,\}$$

We show that given the assumption of a distributive lattice, that if a complement of a exists, then $a \Rightarrow b = \not a \vee b$.