AN INTRODUCTION TO RING THEORY

JOSH ZEITLIN

Abstract

In this paper we will discuss the essence of ring theory and rings, the third major algebraic structure in abstract algebra other than groups and fields. In this paper we will go into depth while studying the topics of rings, homomorphism between rings, a special type of subring called an ideal and quotient rings. Building off of these main topics we will go on to discuss the relationship between all of these concepts and then we'll talk about some major theorems connecting all of these ideas called the three ring isomorphism theorem: the first ring isomorphism theorem, the second ring isomorphism theorem and the third ring isomorphism theorem.

1. Preliminary Definitions

First, we'll start with the definitions of a ring which can be extended from the definition of a group.

Definition 1.1. A ring R is a set of numbers equipped with two binary operations $(+, \cdot)$ and sometimes denoted as $(R, +, \cdot)$ has the following properties:

- The operations $+$ is commutative
- The operations $+$ and $\cdot$ are associative
- Multiplication distributes over addition
- There exists an additive identity element
- There exists a multiplicative identity element
- The multiplicative and additive
- There exists an additive inverse element in the ring for every element in the ring, meaning that $\forall r \in R$ we get that there exists an element $-r$ such that $r + (-r) = 0$.

As you notice this does not require R to have commutativity of multiplication. We now define a ring in which multiplication is commutative.

Definition 1.2. A ring R is called a commutative ring if the operation of multiplication, denoted $\cdot$, is a commutative operation.

Let's now look at a few examples of rings.

Example. The integers, $\mathbb{Z}$ is a ring under addition and multiplication.

Example. The integers modulo n where $n \in \mathbb{N}$ forms a ring.

Example. The rational numbers, $\mathbb{Q}$ forms also forms a ring under addition and multiplication

Example. We also have the real numbers $\mathbb{R}$

Example. And of course we have the complex numbers, $\mathbb{C}$ also form a ring.

Example. All polynomials with integral coefficients form a ring. This ring is denoted $\mathbb{Z}[x]$

Example. The Gaussian Integers, denoted $\mathbb{Z}[i]$ forms a ring. This is the set of the form $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$

From now on, all the rings which we will deal with will be commutative rings so when ring is written assume that it is commutative.

Now, we know that we can add, subtract and multiply elements in a ring but the real question is whether or not we can divide. We know that in fields, we have the property that every element has an inverse which means we can divide, but inverses are not an axiom for rings. Some elements in rings do have inverses but not all, otherwise it would be a field. We'll now define the types of elements of rings that have an inverse.

Definition 1.3. An element of a ring R, $r \in R$ is referred to as a unit if there exists an element r' such that $rr' = 1$ where 1 is the multiplicative identity (and 1 will be the multiplicative identity from now on in this paper). From now on we will also call this element r' to be r^{-1}

Now I'll move on to a few basic propositions that are important to discuss when analyzing rings. For these following propositions, R will denote a commutative ring and r will be a place holder for every element of R.

Proposition 1.4. $\forall r \in R$, $0 \cdot r = r \cdot 0 = 0$

Proof. We see that $r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0$ so thus $r \cdot 0 = r \cdot 0 + r \cdot 0$ and then $r \cdot 0 + (-r \cdot 0) = r \cdot 0 + (r \cdot 0 + (-r \cdot 0))$ and thus $0 = r \cdot 0$ and by commutativity of a ring we get that $r \cdot 0 = 0 \cdot r = 0$ for all $r \in R$. ■

Proposition 1.5. *The element* 1 *(multiplicative identity) is unique. This means that given an element* 1 *such that* $\forall r \in R$ *we get that* $1 \cdot r = r \cdot 1 = r$ *and* $1'$ *such that the same property holds, it must follow that* $1 = 1'$.

Proof. We know that $1 \cdot 1' = 1'$ and because we know that $1'$ is also the identity we get that $1 \cdot 1' = 1$ so we get that $1 \cdot 1' = 1 = 1'$ hence proving that the multiplicative identity is unique. ■

Proposition 1.6. *Just like in fields,* $\forall r_1, r_2 \in R$ *we have that* $-(r_1 \cdot r_2) = (-r_1) \cdot r_2 = r_1 \cdot (-r_2)$

Proof. We know that $r_1 + (-r_1) = 0$ so applying the rule of distributivity we have that $r_2(r_1 + (-r_1)) = r_2 \cdot 0$ which equals 0 by proposition 1.4. This means that $r_1r_2 + (-r_1)r_2 = 0$ so thus by adding $-(r_1r_2)$ to both sides we get that $(-r_1)r_2 = -(r_1r_2)$. We can apply a similar argument to get $r_2 + (-r_2) = 0$ and then by distributivity and prop 1.4 we get that $r_1(r_2 + (-r_2)) = 0$ and thus $r_1r_2 + r_1(-r_2) = 0$ so by adding $-(r_1r_2)$ to both sides we'll get that $r_1(-r_2) = -(r_1r_2)$ so we end up getting that $r_1(-r_2) = (-r_1)r_2 = -(r_1r_2)$. ■

Proposition 1.7. $(-1) \cdot (-1) = 1$

Proof. We know that $1 + (-1) = 0$ and thus $(1 + (-1))(1 + (-1)) = 0$ so we get that $1 \cdot 1 + 1 \cdot (-1) + 1 \cdot (-1) + (-1) \cdot (-1) = 0$. Then we get that $(1 + (-1)) + (-1) + (-1) \cdot (-1) = 0$ and then we get that $0 + (-1) + (-1) \cdot (-1) = 0$ and then $1 = (-1) \cdot (-1)$ by adding 1 to both sides. ■

Proposition 1.8. *The element* 0 *(additive identity) is unique*

Proof. Assume for the sake of contradiction that there exists two additive identities called 0 and $0'$ so we get that $0 + 0' = 0'$ but we also get that $0 + 0' = 0$ so then we'd get that $0 = 0'$ proving that the additive identity is unique. ■

Proposition 1.9. *Additive inverses are unique.*

Proof. Assume for the sake of contradiction that given $r \in R$ we have multiple additive inverses, say $-r$ and $(-r)'$. This means that $r + (-r) = r + (-r)' = 0$. Now, adding $-r$ to both sides we get that $r + (-r) + (-r) = -r = -r + r + (-r)' = -r$ so thus we get that $-r = (-r)'$. ■

Proposition 1.10. *For any $r \in R$ we get that $(-1) \cdot r = -r$*

Proof. We know that $r \cdot 0 = 0$ so we get that $r(1 + (-1)) = 0$ and thus $r + (-1) \cdot r = 0$ and thus because additive inverses are unique we get that $(-1) \cdot r = -r$. ■

Now, we understand the basic properties of rings and how they work. Hence, we can move on to looking at subrings and more advanced applications and properties of rings.

2. Subrings

In this section we will define the notion of a subring which is a ring that is a subset of another ring.

Definition 2.1. A subring $S \subseteq R$ of a ring R is a subset of R which is a ring under the same operations as R.

We can expand this definition to the subring test which tests if a given subset of a ring is actually a subring.

Proposition 2.2. *A nonempty subset $S \subseteq R$ is a subring if given $a, b \in S$ we get that $a-b \in S$ and $a \cdot b \in S$*

Now, let's prove this using the ring axioms.

Proof. ■

Let's now look at a few examples of subrings of a given ring R and then analyze their properties.

Example. The even integers (all multiples of 2), denoted $2\mathbb{Z}$ forms a subring of the integers, $\mathbb{Z}$.

Example. The set of all multiples of n, $n\mathbb{Z}$ forms a subring of $\mathbb{Z}$ just like how $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

Example. The set $\mathbb{Z}[i]$ forms a subring of $\mathbb{Q}[i]$

Example. We get that the set $\mathbb{Z}[\frac{1}{2}]$ is a subring of $\mathbb{Q}$

Example. That last example follows from the fact that $\mathbb{Z}$ also forms a subring of $\mathbb{Q}$

Example. We get that $\mathbb{Q}$ is a subring of $\mathbb{R}$.

Example. We then get that $\mathbb{R}$ is a subring of $\mathbb{C}$.

Example. It follows from the past three examples using the transitive property that $\mathbb{Z}$ is a subring of $\mathbb{C}$ as well.

Proposition 2.3. *If A and B are two subrings of R then it is true that $A \oplus B$ is a subring of R as well where $A \oplus B = \{a + b : a \in A, b \in B\}$*

Proposition 2.4. *The intersect of two subrings of a ring form another subring. Another way to frame this is given subrings of R, S_1 and S_2 we have that $S_1 \cap S_2$ is a subring of R.*

Remark 2.5. Is it true that given a ring and two subrings that it follows that the union of those two subrings is also a subring?

3. Ideals

In this chapter, we'll define the notion of an ideal, a special type of subring.

Definition 3.1. A left ideal is any subring I of a ring R such that for every $r \in R$ and $a \in I$ we have that $r \cdot a \in I$ and also for any $a, b \in I$ we have that $a - b \in I$ and also $0 \in I$.

A right ideal is defined the same way but because we are using commutative rings in this paper we won't really need that notion. All of our ideals are what are usually referred to as two-sided ideals.

Now, we'll define the notion of a principal idea.

Proposition 3.2. *Given an element $r \in R$ we say that all of the multiples of r form an ideal which is denoted $\langle r\rangle$ or (r) and is the called principal ideal generated by r or just the ideal generated by r.*

Proof. Any element in $\langle r\rangle$ takes the form ar where $a \in R$. We know from our definition of ideals that this set satisfies the properties of closure under multiplication purely by the definition of how the set is defined. We can also see that if we take two elements in $\langle r\rangle$ that the difference takes the form $ar - br$ and can be factored by distributivity into the form $r(a - b)$ which by definition of $\langle r\rangle$ is going to be in $\langle r\rangle$ which gives us full proof that $\langle r\rangle$ or the principal ideal generated by r is indeed an ideal. ■

Definition 3.3. In a ring in which every ideal is principal, we call that ring a principal ideal ring or a principal ideal domain.

Now let's look at an interesting proposition about how ideals work.

Proposition 3.4. *If the identity $1 \in I$ where I is an ideal then $I = R$*

Proof. Once thinking about this this seems pretty easy to prove. If $1 \in I$ then for every $r \in R$ we get that $r \cdot 1 \in I$ which means that $r \in I$ which thus means that $R = I$ because every element of $R \in I$ and it is impossible for I to contain R as by definition, I is a subring of R. ■

4. Quotient Rings

If we look at what I is in R and just take those to sets under addition, we get the analogue of how a normal subgroup works with respect to a group.

So if we take $r \in R$ and our ideal I we can look at the set $r + I = \{r + i : r \in R, i \in I\}$

This means that $r_1 \equiv r_2 \mod I$ if and only if $r_1 - r_2 \in I$. Let's try and prove this more formally.

Proposition 4.1. *Let R be a ring and I be an ideal of R. Let $r_1 + I$ and $r_2 + I$ denote two cosets of I and we have that $r_1 + I = r_2 + I$ if and only if $r_1 - r_2 \in I$ and we also get that if $r_1 + I \neq r_2 + I$ then $r_1 + I \cap r_2 + I = \{\}$ or in other words, they are disjoint.*

Proof. First we prove that if $r_1+I = r_2+I$ then $r_1 \simeq r_2 \mod I$ or $r_1-r_2 \in I$. If $r_1+I = r_2+I$ then there exist elements $i_1, i_2 \in I$ such that $r_1 + i_1 = r_2 + i_2$ and because $i_1, i_2 \in I$ we know that $i_2 - i_1 \in I$ so $r_1 - r_2 = i_2 - i_1$ so we get that $r_1 - r_2 \in I$ and thus $r_1 \simeq r_2 \mod I$. Going the other direction we get that if $r_1 \simeq r_2 \mod I$ we get that $r_1 - r_2 \in I$ which means that $r_1 - r_2 = i$ which proves that $r_1 = i + r_2$ or $r_1 \in r_2 + I$ and a similar operation in the other direction shows that $r_2 \in r_1 + I$ proving that $r_1 + I = r_2 + I$ through some more simple manipulation.

Next to prove the other part we will assume that $r_1 + I$ and $r_2 + I$ are neither equal nor disjoint, so say $a \in r_1 + I$ and $a \in r_2 + I$. Because $a \in r_1 + I$ we have that $a = r_1 + i_1$ where $i_1 \in I$ and $a = r_2 + i_2$ where $i_2 \in I$ which means that $r_1 + i_1 = r_2 + i_2$ which means that $r_1 - r_2 = i_2 - i_1$ so we get that $r_1 \simeq r_2 \mod I$ which proves that $r_1 + I = r_2 + I$ proving that they is either disjoint or equal. ■

Now, we know from group theory that R/I denotes the set of cosets $\{r + I : r \in R\}$ where our operation is defined by $I + r_1 + I + r_2 = I + (r_1 + r_2)$ which gives us a ring structure on R/I.

Theorem 4.2. *If I is an ideal of $(R, +, \cdot)$ under the operations*

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

$$(r_1 + I)(r_2 + I) = r_1r_2 + I$$

and R/I forms a ring under these operations and we call this ring a quotient ring. Some mathematicians refer to this as a factor ring.

Proof. Let's go through the ring axioms and see if this meets the structural requirements of a ring. But before we do that we have to show that the operations of addition and multiplication are well defined. Addition is a relatively easy proof. For this we assume that $r_1 + I = r_1' + I$ and $r_2 + I = r_2' + I$ where these are our four cosets (two unique) we get that $r_1 + r_2 + I = r_1' + r_2' + I$. This means that $r_1 - r_1' = i_1 \in I$ and $r_2 - r_2' = i_2 \in I$ which means that $r_1 + r_2 - (r_1' + r_2') = i_1 - i_2 \in I$ proving that $(r_1 + r_2) - (r_1' + r_2') \simeq 0 \mod I$ by our other proposition this proves that $r_1 + r_2 + I = r_1' + r_2' + I$.

Now, proving that multiplication is well defined we get that $r_1 + I = r_1' + I$ and $r_2 + I = r_2' + I$ proving that $r_1 - r_1' = i_1 \in I$ and $r_2 - r_2' = i_2 \in I$. Multiplying $r_1'r_2'$ we get that $r_1'r_2' = (i_1+r_1)(i_2+r_2) = i_1i_2+r_1i_2+r_2i_1+r_1r_2$ which gives us $r_1'r_2'-r_1r_2 = i_1i_2+r_1i_2+r_2i_1 \in I$ and thus $r_1'r_2' + I = r_1r_2 + I$ proving that multiplication of cosets is well defined.

Now that this is proved it is relatively easy to look through the ring axioms and just simplify our results with respect to the ideals proving that the set R/I has the structure of a ring. ■

Example. An ideal of $\mathbb{Z}_6$ is the ideal generated by 2, $\langle 2\rangle$ and taking $\mathbb{Z}_6/\langle 2\rangle$ which becomes $\{\langle 2\rangle, 1 + \langle 2\rangle\}$ which equals $\{\{0, 2, 4\}, \{1, 3, 5\}\}$.

Example. Another example of a quotient ring is $\mathbb{Z}/\langle n\rangle$ where $n \in \mathbb{Z}$ and $\langle n\rangle$ is the ideal generated by n. This becomes the set $\{\langle n\rangle, 1 + \langle n\rangle, \cdots n - 1 + \langle n\rangle\}$ and $n + \langle n\rangle = 0 + \langle n\rangle = n$ showing us that $\mathbb{Z}/\langle n\rangle \simeq \mathbb{Z}_n$

5. Ring homomorphisms and Isomorphism theorems

Just like how we have an idea of homomorphisms between groups, we can create a similar operation between rings.

Definition 5.1. Given two rings $(R, +, \cdot)$ and $(S, \oplus, \otimes)$ then a ring homomorphism $f : R \to S$ has the following properties given $a, b \in R$:

- $f(a + b) = f(a)(b)$
- $f(a \cdot b) = f(a) \otimes f(b)$
- $f(1_R) = 1_S$ where 1_R and 1_S are the respective identities for each ring

A ring isomorphism is an isomorphism between rings where the homomorphism is a bijection.

Proposition 5.2. *$\forall r \in R$ we have that $f(-r) = -f(r)$*

Proposition 5.3. *Given $0_R \in R$ we get that $f(0_R) = 0_S$*

Now, let's define the ideas of kernels and images of a morphism.

Definition 5.4. Given a ring homomorphism $f : R \to S$ we get that the kernel of f is $\text{Ker}f = \{r : f(r) = 1_S\}$.

Proposition 5.5. *$Kerf$ is a subring of R*

Proposition 5.6. *$Kerf$ is an ideal of R*

Definition 5.7. The image of a ring homomorphism $f : R \to S$ is defined by $\text{im}f = \{s : f(r) = s \forall r \in R\}$, so every element that is in the set of outputs of the morphism.

Proposition 5.8. *We have that imf is a subring of S*

Now we'll look at the three most important theorems of ring theory.

The first theorem is called the first ring isomorphism theorem.

Theorem 5.9. *If $f : R \to S$ is a ring homomorphism we get that $R/Kerf \simeq Imf$*

This next theorem is called the second ring isomorphism theorem.

Theorem 5.10. *If I and J are ideals of a ring R then $I/(I \cap J) \simeq (I + J)/J$*

The final theorem I will show you is the third isomorphism theorem.

Theorem 5.11. *Let I and J be two ideals of the ring R where $J \subseteq I$ then I/J is an ideal of R/J and most importantly $(R/J)/(I/J) \simeq R/I$.*

6. Bibliography

(1) Allenby, R. B. Rings, Fields, and Groups: An Introduction to Abstract Algebra, 2nd ed. Oxford, England: Oxford University Press, 1991.

(2) Ballieu, R. "Anneaux finis; systèmes hypercomplexes de rang trois sur un corps commutatif." Ann. Soc. Sci. Bruxelles. Sér. I 61, 222-227, 1947.

(3) Beachy, J. A. Introductory Lectures on Rings and Modules. Cambridge, England: Cambridge University Press, 1999.

(4) Berrick, A. J. and Keating, M. E. An Introduction to Rings and Modules with K-Theory in View. Cambridge, England: Cambridge University Press, 2000.

(5) Birkhoff, G. and Mac Lane, S. A Survey of Modern Algebra, 5th ed. New York: Macmillian, 1996.

(6) Bronshtein, I. N.; Semendyayev, K. A.; Musiol, G.; and Muehlig, H. Handbook of Mathematics, 4th ed. New York: Springer-Verlag, 2004.

(7) Dresden, G. ”Small Rings.” https://home.wlu.edu/ dresdeng/smallrings/.

(8) Ellis, G. Rings and Fields. Oxford, England: Oxford University Press, 1993.

(9) Fine, B. ”Classification of Finite Rings of Order p2̂.” Math. Mag. 66, 248-252, 1993.

(10) Fletcher, C. R. ”Rings of Small Order.” Math. Gaz. 64, 9-22, 1980.

(11) Fraenkel, A. ”Über die Teiler der Null und die Zerlegung von Ringen.” J. reine angew. Math. 145, 139-176, 1914.

(12) Gilmer, R. and Mott, J. ”Associative Rings of Order p3̂.” Proc. Japan Acad. 49, 795-799, 1973.

(13) Harris, J. W. and Stocker, H. Handbook of Mathematics and Computational Science. New York: Springer-Verlag, 1998.

(14) Itô, K. (Ed.). ”Rings.” §368 in Encyclopedic Dictionary of Mathematics, 2nd ed., Vol. 2. Cambridge, MA: MIT Press, 1986.

(15) Kleiner, I. ”The Genesis of the Abstract Ring Concept.” Amer. Math. Monthly 103, 417-424, 1996.

(16) Knuth, D. E. The Art of Computer Programming, Vol. 2: Seminumerical Algorithms, 3rd ed. Reading, MA: Addison-Wesley, 1998.

(17) Korn, G. A. and Korn, T. M. Mathematical Handbook for Scientists and Engineers. New York: Dover, 2000.

(18) Nagell, T. ”Moduls, Rings, and Fields.” §6 in Introduction to Number Theory. New York: Wiley, pp. 19-21, 1951.

(19) Renteln, P. and Dundes, A. ”Foolproof: A Sampling of Mathematical Folk Humor.” Notices Amer. Math. Soc. 52, 24-34, 2005.

(20) Singmaster, D. and Bloom, D. M. ”Problem E1648.” Amer. Math. Monthly 71, 918-920, 1964.

(21) Sloane, N. J. A. Sequences A027623 and A037234 in ”The On-Line Encyclopedia of Integer Sequences.”

(22) van der Waerden, B. L. A History of Algebra. New York: Springer-Verlag, 1985.

(23) Wolfram, S. A New Kind of Science. Champaign, IL: Wolfram Media, p. 1168, 2002.

(24) Zwillinger, D. (Ed.). ”Rings.” §2.6.3 in CRC Standard Mathematical Tables and Formulae. Boca Raton, FL: CRC Press, pp. 141-143, 1995.

Email address: `jzeitlin36@gmail.com`