Introductino to Rings and Modules

Joshika Chakraverty

June 7, 2020

1 Introduction

Rings and modules are important parts of abstract algebra. In class, we have worked with groups where you can add, subtract, multiply and divide but there are some groups where division messes with the closure aspect. This paper covers the basics about rings, ring homomorphisms, and modules.

2 Rings

Definition 2.1 (Ring)**.** A ring is a group made of a set R with two binary operations of multiplication, $\times$ and addition $+$.

For any three elements $a, b, c \in R$,

1. Rings are an abelian group under addition. The identity element under addition is written as 0, even though it may not actually be 0.

2. In a ring multiplication is associative, meaning that $a \times b = b \times a$. The ring is also closed under multiplication.

3. Multiplication is distributive over addition. $a \times (b + c) = (a \times b) + (a + b)$, $(a + b) \times c = (a \times b)(a \times c)$

A ring does not have to be commutative under multiplication, but if it is then we can call it a **commutative ring**. Rings do not have to have a multiplicative identity but if it does then it is written as 1 and the ring is called a **Ring with Identity**.

Definition 2.2 (Units)**.** Let R be a ring. $x \in R$ is a **unit** if it has an inverse $a^{-1} \in R$ such that $a \times a^{-1} = 1$ and $a^{-1} \times a = 1$ where 1 is the inverse under multiplication.

In other words, units are the elements that have an inverse under multiplication. The set of units is a group called R^x.

Example. $\mathbb{Z}$ is a commutative ring. The elements with multiplicative inverses are $1, -1$. All other integers would have a fractional inverse which would not be in the set. Thus, $\mathbb{Z}^x = 1, -1$.

Multiplying any integer by a unit gets it's **Associate**. For the ring $\mathbb{Z}$, one example is that 2×-1 is an associate. This idea can help generalize the Fundamental Theorem of Algebra to negative numbers.

Definition 2.3 (Division Ring)**.** A ring is a **division ring** when all the nonzero elements are units.

A division ring is basically a field without commutative multiplication.

Definition 2.4 (Zero Divisors)**.** Let R be a ring. $x \in R$ is a **left zero divisor** if there exists an $a \in R$ such that $xa = 0$ and $a \neq 0$.

A **right zero divisor** can be defined in the same way but the element has to be on the right. A zero divisor can be both a left zero divisor and a right zero divisor. A zero divisor can never be a unit.

Example. Take the ring $R = \mathbb{Z}_n$. An element k has a multiplicative inverse only if $\gcd(n, k) = 1$. This means that it is only a unit if it is relatively prime to the modulus. An element k is a zero divisor if $(n, k) \geq 2$.

Definition 2.5 (Integral Domain)**.** A commutative ring where the multiplicative identity and additive identity are different is an **integral domain** is it has no zero divisors.

An integral domain is is basically a field with no inverses.

The definition of a ring can be applied to some number theory formulas that people take for granted.

Definition 2.6 (Fundamental Theorem of Algebra)**.** Any integer $n \geq 1$ can be uniquely factored into a product of prime numbers.

1 is a unit so it does not count. This is tricky with negative numbers since the negative sign can be latched onto any prime factor. For example, -20 can be factored into $-2 \times 5 \times 2$ or $-5 \times 2 \times 2$ or even $-5 \times -2 \times -2$. Since -2 and 2 are associates and -5 and 5 are associates they can all be matched together. They magnitude and amount of the prime factors are the same, so the prime factorization can be considered unique up to the number of associates.

3 Examples of Rings

Here are some examples of rings that are important to know about because of how common they are:

3.1 Zero Ring

This ring only contains the element 0. This is a finite comm mutative ring. Since there is only one element, it is both the multiplicative and the additive identity.

3.2 Trivial Ring

This ring takes any associative abelian group and defines multiplication as $ab = 0$ for all $a \in R$. In this ring, every elements that is 0 is a left and ring zero divisor so this cannot be a division ring.

3.3 $2\mathbb{Z}$

This set of even integers is a commutative ring under addition and multiplication. There is no multiplicative identity so it cannot be a division ring or an integral domain.

3.4 Polynomial Ring

Chose a commutative ring R. $R[x]$ represents the set of polynomials with coefficients in R. This makes $R[x]$ also a commutative ring. $R[x]$ behaves a lot like R. If there are units in R, the same elements are units in $R[x]$ and if R is an integral domain that means that $R[x]$ is also an integral domain.

3.5 Matrix Ring

Chose a ring R and a positive integer n. $M_n(R)$ is the set of $n \times n$ matrices with elements from R. If R is not zero and $n \geq 2$, the ring has zero divisors and is not commutative even though R may be. If R has a multiplicative identity, the identity matrix has 1's across the diagonal and 0's everywhere else.

3.6 Hamilton Quaternion

This unit quaternion group is $Q_8 = \langle i, j, k \| i^2 = j^2 = k^2 = -1, ij = k \rangle$. Allowing addition turns this group into a ring $\mathbb{H}$ where $\mathbb{H} = \{a + bi + cj + dk \| a, b, c, d \in \mathbb{R}\}$. This ring is isomorphic to the ring $M_4(\mathbb{R})$.

4 Ideals and Quotient Rings

Many group theory concepts can be transferred over to ring theory in order to allow similar operations. For example, groups have subgroups and rings have subrings.

Definition 4.1 (Subring)**.** If R is a ring and S is a subset, then S is only a **subring** if it keeps the structure of a ring, so $0, 1 \in S$, S must be closed under addition and multiplication.

Here are some examples of subrings: $\mathbb{Z}$ is a subring of $\mathbb{R}$ which is a subring of $\mathbb{Q}$. Any prime number n times $\mathbb{Z}$ is a subring of $\mathbb{Z}$. If R is a set of constant functions, it is a subring of $R[x]$.

Ideals can be thought of as the normal subgroups of rings. A normal subgroup of a group divides the group into cosets.

Definition 4.2 (Normal Subgroup)**.** Let G be a group and N be a subgroup. N is a normal subgroup if $g^{-1}Ng \in N$ for all $g \in G$.

The normal subgroup divides the group into cosets, which in turn form their own group called the quotient group. When the group is abelian, every subgroup is normal. An ideal can be defined in a similar fashion.

Definition 4.3 (Ideal)**.** Let R be a ring and $I \leqslant R$ (subgroup). For any $r \in R$ and $x \in I$, $x \times r \in I$ and $r \times x \in I$. We write $I \trianglelefteq R$.

The ideal is a normal subgroup under addition and is closed under multiplication nad would be a subring if it had the identity 1. Ideals also have to property of being right, left, and two-sided ideals based on which side the elements from the subring is multiplied. If R is commutative, then all ideals are two sided. The ideal is also a normal subgroup of R under addition and is closed under multiplication. I would be a subring if it was guaranteed to have 1 in it. One example of an ideal is $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Example. Under the ring $\mathbb{Z}[x]$, and ideal is $I = x\mathbb{Z}[x]$. I is a subgroup because it is associative, commutative, has the identity, is closed under addition because like terms are added together, and have additive inverses because the coefficients can switch signs. We have to show that for any $f, j \in I$ $fj \in I$ and $jf \in I$. Since the polynomial ring is already commutative, $jf = fj$ so we only have to prove on of them. $j \in I$ can be factored into $x \cdot k$ where k is some other polynomial. $fj = fxk = xfk$ but fk is a polynomial and x times any polynomial is in I so $fj \in I$. This completes the proof that $x\mathbb{Z}[x]\mathbb{Z}$.

Definition 4.4 (Quotient Ring)**.** The ring of cosets R/I form the **quotient ring**.

The structure of the quotient ring is isomorphic the the quotient group of the additive abelian group R by all of its normal subgroups. R/I cannot turn into a ring for any subring I, only for two sided ideals I because the ring needs closure under multiplication.

Here is what happens when subrings are used to try to form a quotient ring: Let I be a subring of ring R. Let $r + I$ and $s + I$ be two cosets. The product of these two cosets have to be independent of their elements so we can define $\alpha, \beta \in I$ where $r + \alpha \in r + I$ and $\beta \in s + I$. Since these elements are in the subring, we should have $(r+\alpha)(s+\beta)+I = rs+I$ for all $r, s \in R$ and $\alpha, \beta \in I$. When $r = s = 0$, $\alpha\beta \in I$. THis

5 Ring Homomorphisms and Isomorphisms

Homomorphisms on rings are very similar to homomorphisms on groups. The homomorphism is a structure preserving map between rings.

Definition 5.1 (Ring homomorphism)**.** Let R and S be rings. A map $f : R \to S$ is a ring homomorphism if

1. $f(1_R) = 1_s$. The multiplicative identity of the first rings maps to identity to the second ring.

2. $f(0_r) = 0_s$. The additive identity of the first ring maps to the additive identity of the second ring.

3. For $r_1, r_2 \in R$ $f(r_1 + r_2) = f(r_1) + f(r_2)$.

4. For $r_1, r_2 \in R$ $f(r_1 \times r_2) = f(r_1) \times f(r_2)$.

The kernel of the ring homomorphism is $\{r \in R \| f(r) = 0\}$.The image of a ring homomorphism is a subring of S. If the subring is the whole ring, then f is surjective. If f is a bijection then f is an **isomorphism**.

Example. Define a function $f : \mathbb{Z} \to \mathbb{Z}$ where $n \geq 2$ as $f_n(x) = nx$. Both the identity clauses hold but we have to check the third and fourth clause. $f_n(x + y) = n(x + y) = nx + ny = f_n(x) + f_n(y)$. However, $f_n(x)f_n(y) = (nx)(ny) = n^2xy$ which does not work for all values of n. This function is only a ring homomorphism when $n = 0, 1$.

Example. Define a ring homomorphism $f : \mathbb{Z} \to \mathbb{Z}_n$ where $f : k \to k(\mod n)$. $\ker(f) = n\mathbb{Z}$ which includes all multiples of n. This ring homomorphism is not one-to-one but it is onto.

Example (Evaluator function). This ring homomorphism goes from $\mathbb{Q}[x] \to \mathbb{Q}$ by $f(p(x)) = p(0)$. It plugs in zero into the polynomial and finds the roots of the polynomials. The kernel is the set of polynomials in $\mathbb{Q}$ with constant terms only.

There are a set of isomorphism theorems for rings that describe how homomorphisms, subrings and quotient rings interact with each other.

Theorem 5.2 (Fundamental Homomorphism Theorem)**.** *If $f : R \to S$ is a ring homomorphism, then ker(f) is an ideal and Im(f) $\simeq$ R/ker(f).*

Any homomorphism leads to an image that is a subring of S. The quotient process leads to a quotient ring $R/\ker(f)$, and another isomorphism can relabel that quotient ring into the image. This fundamental theorem is true for the additive group. To prove it, the kernel has to be an ideal and the function $g : R/I \to \text{im}(f)$ defined by $g(x + I) = f(x)$, where I is an ideal and $x \in R/I$, has to be a ring homomorphism.

Theorem 5.3 (Second Isomorphism Theorem for Rings)**.** *If S is a subring and I is an ideal of R*

1. *$S + I = \{s + i | s \in S, i \in I\}$ has to be a subring of R and $S \cap I$ has to be an ideal of S.*

2. *$(S + I)/I \simeq S/(S \cap I)$. Those two quotient groups have to be isomorphic.*

This theorem comes from the fact that $S + I$ is an additive subgroup. It is closed under multiplication because for s_1, s_2§ and $i_1, i_2 \in I$ $(s_1 + i_1)(s_2 + i_2) = s_1s_2 + s_1i_1 + s_2i_1 + i_1i_2$. $s_1s_2 \in S$ and the other three terms are contained in I. It is easy to prove that $S \cap I$ is an ideal of S. $(S + I)/I$ and $S/(S \cap I)$ are both additive groups. One possible isomorphism f is $f : s + (S \cap I) \to S + I$. This sends the identity to itself and follows the other rules that isomorphisms need to follow.

The next isomorphism theorem summarizes how ideals and subrings interact with each other.

Theorem 5.4 (Third Isomorphism Theorem)**.** *This is also known as the freshman theorem. Let R be a ring and $I \trianglelefteq R$.*

1. *If A is a subring of R where $I \subseteq A \subseteq R$, then A/I is a subring of R/I.*
2. *Every subring R/I can be written as A/I for a subring A in R where $I \subseteq A \subseteq R$*
3. *If J is an ideal of R where $I \subseteq J \subseteq R$, J/I is an ideal of R/I.*
4. *every ideal of R/I can be written as A/I for an ideal J in R where $I \subseteq J \subseteq R$.*
5. *If J is an ideal of R where $I \subseteq J \subseteq R$, then $(R/I)/(J/I) \simeq R/J$.*

Theorem 5.5 (Fourth Isomorphism Theorem)**.** *This theorem is also known as the correspondence theorem. If I is an ideal of ring R, there is a bijective correspondence between subrings of R/I and subrings of R that contain I. Every ideal of R/I has the form J/I for some ideal J satisfying $I \subseteq J \subseteq R$.*

6 Modules

Modules are like vector spaces but for rings instead of fields. A vector space has an abelian group of vectors and a field of scalars. The vectors can be scaled by the elements in the field to create new vectors. In a vector space, the distributive property and the associative property both hold. In a module, the field is replaced with a ring and the abelian group has "elements" instead of "vectors"

Definition 6.1 (Module)**.** Let R be a commutative ring. M is a module over R if

1. M is additive abelian group
2. $R \times M \to M$ is a multiplicative action that holds the distributive laws over addition
3. If 1 is the identity of R, $1x = x$ for all $x \in M$

In the definition, the module is a **left-Rmodule** because the ring is multiplied to the left of the module. If the order was switched, then we would have a **right-Rmodule**.

Definition 6.2 (Submodules)**.** Let M be a module over a commutative ring R. $A \subset M$ is a **submodule** if for all $a_1, a_2 \in A$ and $r_1, r_2 \in R$, $r_1x_1 + r_2x_2 \in A$.

Every module M has submodules of M, the whole module, and 0, the zero element. Every abelian group is a $\mathbb{Z}$-module. The following example shows how multiplication is defined.

7 Module Examples

Example. Let M be any abelian group and let the scalars be $\mathbb{Z}$. Scalar multiplication for $r\mathbb{Z}$ and $a \in M$ is defined by the following:

1. $r \geq 0$ $r \cdot a = a + a + ... + a$ where there are r a's multiplied to each other.
2. $r = 0$ $0 \cdot a = 0$ where the left 0 is in $\mathbb{Z}$ and the right 0 is the identity of M.
3. $r \leq 0$ $r \cdot a = -a - a... - a$ where r a's are being subtracted.

Example. Take the group $M = \mathbb{R}^3 = \{(x, y, z)|x, y, z \in \mathbb{R}$, which are three dimensional vectors with real coefficients. Let the scalar ring R be all of the 3×3 matrices with elements in $\mathbb{R}$. R is definitely not a field because there are some matrices that do not have multiplicative inverses. In this case multiplication can be defined as matrix multiplication.

Example (Coordinate Space R^n). Take a commutative ring R and take n elements of R to form a new space. $R = \{(x_1, x_2, ..., x_n)|x_1, x_2, ..., x_n \in R$. This is a module with the same operations of addition and scalar multiplication.

Example (Linear Map over Polynomial Rings). Take a field F and a vector space V over that field. Define $T : V \to V$ to make T a mapping from the vector field to itself that preserves addition and scalar multiplication. T is called a linear map. Adding elements of V is allowed so we have to figure out how to multiple elements of V by elements of $F[x]$. For $f(x) \in F[x]$, let $f(x) \cdot v = f(T)v$. What this does is that is plus T into $f(x)$ and gets another linear map $f(T) : V \to V$. The left side of the equation is the image of v under $f(T)$.

8 Group Rings

Group rings are a kind of like modules except there is a finite multiplicative group rather than an additive abelian group.

Definition 8.1 (Group Ring)**.** Given a commutative ring R and a finite multiplicative group G define multiplication as

$$RG = \{a_1g_1 + a_2g_2 + ... + a_ng_n \| a_i \in R, g_i\}$$

This multiplication just takes elements of each and multiplies them to each other in a straightforward way.

Example. If the ring is $R = \mathbb{Z}$ and the group is $G = D_4 = \langle \rho, \tau | \rho^4 = \tau^2 = \rho\tau\rho\tau = 1 \rangle$. Two elements in this group rings are $x = \rho + \rho^2 - 3\tau$ and $y = -5\rho^2 + \rho\tau$. Adding them together gets:

$$x + y = \rho - 4\rho^2 - 3\rho + \rho\tau.$$

Multiplying them gets:

$$xy = (\rho + \rho^2 - 3\tau)(-5\rho^2 + \rho\tau) = -5\rho^3 + \rho^2\tau - 5\rho^4 + \rho^3\tau + 15\tau\rho^2 - 3\tau\rho\tau.$$

This can be simplified using the fact that a lot of the movements just equal the identity. We end up with

$$xy = -5 - 8\rho^3 + 16\rho^2\tau + \rho^3\tau.$$

Another example is that the Hamiltonian ring $\mathbb{H}$ is not the same ring as $\mathbb{R}Q_4$. The Hamiltonian group has no zero divisors, so the group $\mathbb{R}Q_4$ has more elements that are zero divisors. If an element $g \in G$ has finite order greater than 1, then RG always has zero divisors. RG has a subring that is isomorphic to R and the group of units $U(RG)$ as a subring isomorphic to G.

9 Conclusion

This is a very basic overview of what rings and modules are. There is a lot more to explore, like direct products and sums, injective and projective modules, and quasi-frobenius rings. Ring Theory is an extension of group theory that has a lot of potential for applications in places like physics and cryptography.

References

[1] F. Kasch, *Modules and rings*, vol. 17. Academic Press, 1982.

[2] N. Carter, *Visual group theory*, vol. 32. MAA, 2009.

[3] J. Lambek, *Lectures on rings and modules*, vol. 283. American Mathematical Soc., 2009.