21MAB143 Rings and Polynomials
Week 1

Introduction

Rings are mathematical structures with two "compatible" operations. They provide a common generalisation of, one one hand, familiar number systems such as the integers, and on the other, sets of functions. Studying rings from the general point of view can help us to understand the common features of these seemingly different objects.

In this module we will study rings with a particular focus on one class of examples, namely **polynomial rings**. A polynomial is an algebraic expression built up from one or more variables by multiplication, addition, and scaling by coefficients. Here is an example of a polynomial in one variable (with rational coefficients):

$$x^{19} - \frac{7}{5}x^{11} + 4x^4 - \frac{3}{2}$$

Here is a polynomial in three variables:

$$xy^3z + xy + 2z^2 - 3xz - z + 7$$

Polynomials are used throughout all branches of pure and applied mathematics. For example, numerical algorithms that compute approximate values of transcendental functions such as $\sin$ and $\cos$ are actually working with high-precision polynomial approximations of those functions; as a more extreme example, the entire subject of algebraic geometry is fundamentally based on polynomials and the geometric information they contain.

The goal of this module will be to develop computational methods for polynomials, both in the single-variable and multi-variable cases. We will see that there are significant differences between the two, and we will also develop the theoretical background to unnderstand these differences.

Reading List

The following books are available in the University library. Each of them covers some of the module content (along with many other topics that are not part of this module).

Please note that **my module materials remain the definitive source for the module content.**

1. Peter J. Cameron. *Introduction to Algebra*, various editions. 512.02/CAM
2. John R. Durbin. *Modern Algebra: An Introduction*, various editions. Wiley. 512.02/DUR
3. John B. Fraleigh. *A First Course in Abstract Algebra*, various editions. Pearson. 512.02/FRA
4. Serge Lang. *Undergraduate Algebra*, 3rd ed. Springer. 512/LAN
5. Joseph J. Rotman. A First Course in Abstract Algebra. Pearson/Prentice Hall. 512/ROT

Prerequisites

This module will refer to some material that was covered MAA242 Geometry and Groups, in particular the following concepts:

- group
- abelian group
- group homomorphism
- kernel of a homomorphism

See your Geometry and Groups notes to revise this material. Alternatively you can consult the "MAB143 Week 0" notes on Learn for a brief summary of the relevant ideas, or the Groups lecture notes by Professor Veselov for a more detailed treatment.

1 Rings

A ring is, roughly speaking, a mathematical structure with two "compatible" operations of addition and multiplication. The following definition makes this rough idea precise.

Definition 1.1. *A* **ring** *is a nonempty set R together with two binary operations $+$ (addition) and $\times$ (multiplication) satisfying the following axioms:*

1. *The pair $(R, +)$ is an* **abelian group***, meaning:*

   (a) *Addition $+$ is associative: that is, for any elements a, b, $c \in R$ we have*

   $$a + (b + c) = (a + b) + c.$$

   (b) *Addition $+$ is commutative: for any a, $b \in R$ we have*

   $$a + b = b + a.$$

   (c) *There exists an additive identity element: that is, an element $0 \in R$ such that for all $a \in R$ we have*

   $$0 + a = a.$$

   (d) *For each element $a \in R$ there exists an additive inverse element $-a$ such that*

   $$a + (-a) = 0.$$

2. *Multiplication $\times$ is* **associative***: that is, for any elements a, b, $c \in R$ we have*

   $$a \times (b \times c) = (a \times b) \times c.$$

3. *The two operations satisfy* **distributive laws:** *for any elements a, b, $c \in R$ we have*

   $$\begin{aligned} a \times (b + c) &= a \times b + a \times c \\ (a + b) \times c &= a \times c + b \times c. \end{aligned}$$

4. *There exists a* **multiplicative identity element***: that is, an element $1 \in R$ such that for all $a \in R$ we have*

   $$1 \times a = a \times 1 = a.$$

Axiom 4 is a bit controversial: most sources include it as part of the definition of a ring, but not all do. Since all the rings we will be concerned with in this module do have a multiplicative identity element, it makes sense for us to include this axiom.

These axioms allow us to prove that various familiar "rules" of number systems are still valid in any ring. Here is one example:

Proposition 1.2. *Let R be a ring with additive identity element 0. For any element $a \in R$ we have*

$$a \times 0 = 0 \times a = 0.$$

Proof. See Problem Sheet 1. □

One property we might expect of multiplication is that "order doesn't matter", but note that is not part of our definition. Rings in which we can swap the order of multiplication without changing the result have a special name:

Definition 1.3. *We say that a ring R is* **commutative** *if for all a, $b \in R$ we have*

$$a \times b = b \times a.$$

We'll shortly see familiar examples of rings which are not commutative. However, in this module our focus will be almost exclusively on commutative rings.

As with subgroups of a group, or subspaces of a vector space, we will often consider "subobjects" of a ring. The definition will not be surprising:

Definition 1.4. *Let R be a ring. A subset $S \subset R$ is called a* **subring** *of R if:*

1. *For any elements, a, $b \in S$ we have $a + b \in S$ and $a \times b \in S$.*
2. *For any element $a \in S$ we have $-a \in S$.*
3. *The additive identity element 0 and multiplicative identity element 1 are both in S.*

In other words, a subring of R is a subset of R which is a ring itself under the same operations.

Finally we need to mention one special class of rings, in which "division" is possible:

Definition 1.5. *A* **field** *K is a commutative ring in which every nonzero element has a multiplicative inverse: that is, for all $a \in K$ such that $a \neq 0$, there exists $a^{-1} \in K$ such that*

$$a \times a^{-1} = 1.$$

1.1 Examples

Whenever we encounter an example of a ring, we can ask the following questions:

- Is the ring commutative?
- Is it a field? If not, which elements have multiplicative inverses?
- Can you identify any interesting subrings of the ring?

- Does the ring have any other unexpected properties?

Let's do that with some familiar and important examples of rings.

1. **The integers $\mathbf{Z}$**

   Here the operations are the usual ones: addition $(+)$ and multiplication $(\times)$. Let's think about the questions above:

   - *Commutative?* Yes:

     $$a \times b = b \times a \quad \text{for all } a, b \in \mathbf{Z}$$

   - *Field?* No, because not every element $a \in \mathbf{Z}$ has a multiplicative inverse $a^{-1} \in \mathbf{Z}$. For example consider $2 \in \mathbf{Z}$: there is no integer b such that $2 \times b = 1$.

     Of course 2 has an inverse in the *rational* numbers $\mathbf{Q}$, but the field axioms require an inverse in $\mathbf{Z}$ itself.

   - *Subrings?* If $S \subset \mathbf{Z}$ is a subring, then we must have $1 \in S$. But then S must contain the sums $1+1$ and $1+1+1$ and $1+1+1+\cdots$

     Also S must contain inverses for each of its elements, so we must have $-1 \in S$. But then similarly S must contain $(-1)+(-1)$ and $(-1)+(-1)+(-1)$ and $(-1)+(-1)+(-1)+\cdots$.

     So in fact we must have $S = \mathbf{Z}$.

2. **The rational numbers $\mathbf{Q}$**

   The elements of this ring are fractions $\frac{a}{b}$ where $a, b \in \mathbf{Z}$ and $b \neq 0$.

   The operations are usual addition $(+)$ and multiplication $(\times)$ of fractions.

   - *Commutative?* Yes:

     $$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd} = \frac{c}{d} \times \frac{a}{b}.$$

   - *Field?* Yes: if $\frac{a}{b} \neq 0$ then $a \neq 0$ and

     $$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

   - *Subrings?* One subring is the ring of integers $\mathbf{Z} \subset \mathbf{Q}$: it is a subring since the sum and product of integers is an integer, and $1 \in \mathbf{Z}$.

     There are more interesting subrings too: for example you can check that

     $$S = \left\{ \frac{p}{q} \mid p \text{ and } q \text{ coprime, } q = 2^m \text{ for some } m \right\}$$

     is a subring of $\mathbf{Q}$.

3. **The ring $\mathbf{Z}_n$ of integers modulo n**

   Here we have the set

   $$\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$$

   The operations are $+_n$ (addition mod n) and $\times_n$ (multiplication mod n). It's not too hard to check that this set with these operations satisfies all the ring axioms.

   - *Commutative?* Yes:

     $$\begin{aligned} a \times_n b &= ab \mod n \\ &= ba \mod n \\ &= b \times_n a \end{aligned}$$

   - *Field?* The answer depends on n.
     - If $n = p$, a **prime** number, then $\mathbf{Z}_n$ is a field. (See Problem Sheet 1.)
     - If n is **not** prime, then $\mathbf{Z}_n$ is not a field. For example consider $n = 6$: then

       $$\begin{aligned} 2 \times_6 3 &= 2 \cdot 3 \mod 6 \\ &= 0. \end{aligned}$$

       But in a field, if a and b are nonzero elements, then $a \times b \neq 0$ too. (See Problem Sheet 1). So $\mathbf{Z}_6$ is not a field.

   Remark: We just saw something unexpected: there are rings in which the product of 2 nonzero elements can be equal to zero!

4. **Matrix rings $M_n(\mathbf{R})$**

   Here $M_n(\mathbf{R})$ means the set of $n \times n$ matrices with with real entries. The operations are matrix addition $+$ and matrix multiplication $\times$.

   For this ring we will just focus on one question:

   - *Commutative?* No: for general M, $N \in M_n(\mathbf{R})$ we have

     $$M \times N \neq N \times M$$

     For a concrete example, take $n = 2$ and let

     $$M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad N = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}$$

     Then

     $$\begin{aligned} M \times N &= \begin{pmatrix} 19 & * \\ * & * \end{pmatrix} \\ N \times M &= \begin{pmatrix} 23 & * \\ * & * \end{pmatrix} \end{aligned}$$

     where the entries $*$ are something that doesn't matter.

2 Ring homomorphisms and ideals

As with other kinds of mathematical structures, we are not just interested in rings in isolation, but also in mappings between them that are compatible with the ring operations.

Definition 2.1. *Let R and S be rings. A* **ring homomorphism** *from R to S is a function $f : R \to S$ such that:*

1. *For all elements $a, b \in R$ we have*

$$f(a + b) = f(a) + f(b)$$
$$f(a \times b) = f(a) \times f(b)$$

2. *For the multiplicative identity elements $1_R \in R$ and $1_S \in S$, we have*

$$f(1_R) = 1_S.$$

A ring homomorphism which is also bijective is called an **isomorphism***.*

Definition 2.2. *If $f : R \to S$ is a ring homomorphism, its* **kernel** *is defined as*

$$\mathrm{Ker}(f) = \{r \in R \mid f(r) = 0_S\}$$

and its **image** *is defined as*

$$\mathrm{Im}(f) = \{s \in S \mid s = f(r) \textit{ for some } r \in R\}.$$

In the Geometry and Groups module you saw that the kernel of a group homomorphism is always a **normal subgroup**, and conversely given a normal subgroup N of a group G, there is a group homomorphism from G to another group whose kernel is exactly N. Let's introduce the corresponding notions for rings. From now on, we will stick almost exclusively to commutative rings.

Definition 2.3. *An* **ideal** *I in a commutative ring R is a subset $I \subset R$ such that*

1. *The subset I is nonempty.*
2. *The subset I is closed under addition: that is, for all $a, b \in I$ we have $a + b \in I$ also.*
3. *For any element $a \in I$ and any element $r \in R$, we have $r \times a \in I$.*

Proposition 2.4. *Let R be a commutative ring and $f : R \to S$ a homomorphism to another ring. Then the kernel $\mathrm{Ker}(f)$ is an ideal of R.*

Proof. We have to prove that $\mathrm{Ker}(f)$ satisfies the 3 axioms in Defintion 2.3.

1. Since $f(0_R) = 0_S$, the element 0_R belongs to $\mathrm{Ker}(f)$, so it is nonempty.

2. For two elements a, $b \in \mathrm{Ker}(f)$, we have

$$\begin{aligned} f(a+b) &= f(a)+f(b) \\ &= 0_s + 0_s \\ &= 0_s \end{aligned}$$

so $a+b \in \mathrm{Ker}(f)$ also. Hence $\mathrm{Ker}(f)$ is closed under addition.

3. Suppose $a \in \mathrm{Ker}(f)$ and $r \in R$. Then

$$\begin{aligned} f(r \times a) &= f(r) \times f(a) \\ &= f(r) \times 0_S \\ &= 0_S. \end{aligned}$$

□

The converse statement is also true, as we'll now see.

Definition 2.5. *Let R be a ring and $I \subset R$ a subring. Let $a \in R$ be any element. The* **coset of I containing a** *is the subset $I + a \subset R$ defined by*

$$I + a = \{r + a \mid r \in I\}.$$

The set of all cosets of I in R is denoted R/I.

Proposition 2.6. *Let R be a commutative ring and $I \subset R$ an ideal. Define two operations $+$ and $\times$ on the set of cosets R/I as follows:*

$$\begin{aligned} (I+a)+(I+b) &= I+(a+b) \\ (I+a)\times(I+b) &= I+(a\times b). \end{aligned}$$

These operations make R/I into a ring with additive identity $I+0$ and multiplicative identity $I+1$. The map

$$\begin{aligned} q : R &\rightarrow R/I \\ a &\mapsto I + a \end{aligned}$$

is a surjective ring homomorphism with

$$\mathrm{Ker}(q) = I.$$

Remark: Why do we need to take I to be an **ideal** in the statement of the theorem? On Problem Sheet 1 you will show this ensures that the multiplication operation on R/I is well-defined.

We will finish by stating the counterpart for rings of the Homomorphism Theorem for groups from the Geometry and Groups module. The proof is very similar, and we will not give it here. Before stating it, we need a preparatory result.

Proposition 2.7. *Let* $f : R \to S$ *be a ring homomorphism. Then its image* $\mathrm{Im}(f)$ *is a subring of* S*.*

Proof. See Problem Sheet 1. □

Theorem 2.8 (Homomorphism Theorem for Rings)**.** *Let* $f : R \to S$ *be a ring homomorphism. Let* $K = \mathrm{Ker}(f)$ *be the kernel of* f*, and let* $I = \mathrm{Im}(f)$ *be the image of of* f*. Then* f *induces a ring isomorphism*

$$\begin{aligned} \tilde{f}\colon R/K &\cong I \\ K + a &\mapsto f(a). \end{aligned}$$

2.1 Examples

1. **Homomorphisms from $\mathbf{Z}$**

   Let R be a a ring with multiplicative identity 1_R. Let $f\colon \mathbf{Z} \to R$ be a ring homomorphism. Then we have

   $$\begin{aligned} f(0) &= 0_R \\ f(1) &= 1_R \end{aligned}$$

   So for any integer $k > 0$ we have

   $$\begin{aligned} f(k) &= f(1 + \cdots + 1) \\ &= f(1) + \cdots + f(1) \\ &= 1_R + \cdots + 1_R \end{aligned}$$

   where each $\cdots$ indicates that we are adding k times.

   Also

   $$\begin{aligned} f(k) + f(-k) &= f(k + (-k)) \\ &= f(0) \\ &= 0_R \end{aligned}$$

   so we have $f(-k) = -f(k)$. Therefore

   $$\begin{aligned} f(-k) &= -f(k) \\ &= -(1_R + \cdots + 1_R). \end{aligned}$$

   So this means that f is uniquely determined by the axioms: in other words, there is a **unique** homomorphism from $\mathbf{Z}$ to R.

Example: For a concrete example, take $R = \mathbf{Z}_n$. Then the only ring homomorphism $\mathbf{Z} \to \mathbf{Z}_n$ is reduction mod n:

$$\begin{aligned} \rho_n \colon \mathbf{Z} &\to \mathbf{Z}_n \\ k &\mapsto k \mod n \end{aligned}$$

Its kernel is

$$\begin{aligned} \mathrm{Ker}(\rho_n) &= \{k \in \mathbf{Z} \mid \rho_n(k) = 0\} \\ &= n\mathbf{Z}. \end{aligned}$$

2. **Complex conjugation**

We claim that complex conjugation

$$\begin{aligned} \gamma \colon \mathbf{C} &\to \mathbf{C} \\ x + iy &\mapsto x - iy \end{aligned}$$

is a ring homomorphism. We need to check the axioms:

- $\gamma(1) = 1$: this is clear.
- For all z_1, $z_2 \in \mathbf{C}$ we have $\gamma(z_1 + z_2) = \gamma(z_1) + \gamma(z_2)$. I will leave this as an exercise.
- For all z_1, $z_2 \in \mathbf{C}$ we have $\gamma(z_1 z_2) = \gamma(z_1)\gamma(z_2)$. To see this, write

$$\begin{aligned} z_1 &= x_1 + iy_1 \\ z_2 &= x_2 + iy_2 \end{aligned}$$

Then

$$\begin{aligned} z_1 z_2 &= (x_1 + iy_1)(x_2 + iy_2) \\ &= (x_1 x_2 - y_1 y_2) + i(x_i y_2 + x_2 y_1) \end{aligned}$$

so

$$\gamma(z_1 z_2) = (x_1 x_2 - y_1 y_2) + i(x_i y_2 + x_2 y_1).$$

On the other hand we have

$$\begin{aligned} \gamma(z_1)\gamma(z_2) &= (x_1 - iy_1)(x_2 - iy_2) \\ &= (x_1 x_2 - y_1 y_2) + i(x_i y_2 + x_2 y_1) \end{aligned}$$

So we have $\gamma(z_1 z_2) = \gamma(z_1)\gamma(z_2)$ as required.

Note that

$$\begin{aligned}\mathrm{Ker}(\gamma) &= \{z \in \mathbf{C} \mid \gamma(z) = 0\}\\ &= \{0\}.\end{aligned}$$

In fact, since $\mathbf{C}$ is a field, the only ideals in $\mathbf{C}$ are $\{0\}$ and $\mathbf{C}$ itself. So if $f \colon \mathbf{C} \to R$ is any ring homomorphism to any ring R, then either its kernel is $\{0\}$ or else f is injective.

3. **The polynomial ring $\mathbf{R}[x]$** The elements of this ring are polynomials

$$f = a_n x^n + \cdots + a_1 x + a_0$$

where the coefficients a_i are real numbers.

Now fix a real number $r \in \mathbf{R}$ and define the set

$$I_r = \{f \in \mathbf{R}[x] \mid f(r) = 0\}.$$

I claim that I_r is an ideal. To see this, we have to show for example that if $f \in I_r$ and $g \in \mathbf{R}[x]$ then $gf \in I_r$. But this is easy:

$$\begin{aligned}(gf)(r) &= g(r)f(r)\\ &= g(r) \cdot 0\\ &= 0.\end{aligned}$$

We can define a map

$$\begin{aligned}\mathrm{ev}_r \colon \mathbf{R}[x] &\to \mathbf{R}\\ f &\mapsto f(r)\end{aligned}$$

Next week we'll prove this is a ring homomorphism. Taking that as given for now, the kernel is

$$\begin{aligned}\mathrm{Ker}(\mathrm{ev}_r) &= \{f \in \mathbf{R}[x] \mid f(r) = 0\}\\ &= I_r.\end{aligned}$$

It's also not hard to check that ev_r is surjective, so the Homomorphism Theorem for rings tells us that

$$\frac{\mathbf{R}[x]}{I_r} \cong \mathbf{R}.$$

Next week we'll see a concrete description of the ideal I_r: in fact

$$I_r = \{f \in \mathbf{R}[x] \mid f = (x - r)g \text{ for some } g \in \mathbf{R}[x]\}.$$