14. Rings

We introduce the main object of study for the second half of the course.

Definition 14.1. *A* **ring** *is a set R, together with two binary operations addition and multiplication, denoted $+$ and $\cdot$ respectively, which satisfy the following axioms. Firstly R is an abelian group under addition, with zero as the identity.*

(1) (Associativity) For all a, b and c in R,

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

(2) (Zero) There is an element $0 \in R$ such that for all a in R,

$$a + 0 = 0 + a.$$

(3) (Additive Inverse) For all a in R, there exists $b \in R$ such that

$$a + b = b + a = 0.$$

b will be denoted $-a$.

(4) (Commutavity) For all a and b in R,

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

Secondly multiplication is also associative and there is a multiplicative identity 1.

(5) (Associativity) For all a, b and c in R,

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

(6) (Unit) There is an element $1 \neq 0 \in R$ such that for all a in R,

$$a \cdot 1 = 1 \cdot a.$$

Finally we require that addition and multiplication are compatible in an obvious sense.

(7) (Distributivity) For all a, b and c in R, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Unfortunately there is no standard definition of a ring. In particular some books do not require the existence of unity, or if they do require it, then they do not necessarily require that it is not equal to zero.

Example 14.2. *The complex numbers $\mathbb{C}$ form a ring, with the obvious multiplication and addition.*

Definition 14.3. *Let R be a ring and let S be a subset. We say that S is a **subring** of R, if S becomes a ring, with the induced addition and multiplication.*

Lemma 14.4. *Let R be a ring and let S be a subset that contains* 1.

Then S is a subring iff S is closed under addition, additive inverses and multiplication.

Proof. Similar proof as for groups. ☐

Note that we require S to contain 1. Since we don't necessarily have multiplicative inverses, just because S is non-empty, does not force S to contain 1.

Example 14.5. *The following tower of subsets*

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

is in fact a tower of subrings. A more interesting example is given by taking all rational numbers of the form a/b, where a and b are integers and b is odd. This set is a subring of the rational numbers. Indeed it contains 1 *and it is easy to see that it is closed under addition and multiplication.*

Finally consider the Gaussian integers, defined as all complex numbers of the form

$$a + bi,$$

where a and b are integers. It is easy to see that the Gaussian integers form a subring of the complex numbers.

Example 14.6. *Let $\mathbb{Z}_n$ denote the left cosets of $n\mathbb{Z}$ inside $\mathbb{Z}$, or what comes to the same thing, the integers modulo n. We showed that the law of addition and multiplication descends from $\mathbb{Z}$ down to $\mathbb{Z}_n$. With these rules of addition and multiplication, $\mathbb{Z}_n$ becomes a ring. Indeed* $[0]$ *plays the role of zero and* $[1]$ *plays the role of the identity. In fact we proved that $\mathbb{Z}_n$ is a group under addition and it is not much more work to prove that $\mathbb{Z}_n$ is in fact a ring. Moreover we will see later that this is an example of a much more general phenomena.*

It is interesting to see what happens in a specific example. Suppose that $n = 6$. In this case $0 = [0]$ and $1 = [1]$. However note that one curious feature is that

$$[2][3] = [2 \cdot 3] = [6] = [0],$$

so that the product of two non-zero elements of R might in fact be zero.

Definition-Lemma 14.7. *Let X be any set and let R be any ring. Then the set R of functions from X into R becomes a ring, with addition and multiplication defined pointwise. That is to say, given f and $g \in R$, define $f + g$ by the rule,*

$$(f + g)(x) = f(x) + g(x) \in R,$$

where $x \in X$ and addition is in R. Similarly define the product $f \cdot g$ of f and g by the rule,

$$(f \cdot g)(x) = f(x) \cdot g(x) \in R.$$

Then the zero function f, defined by the rule

$$f(x) = 0 \in R,$$

for all $x \in X$, plays the role of zero and the function g, defined by the rule

$$g(x) = 1 \in R,$$

plays the role of 1.

Proof. Again, all of this is easy to check. We check associativity of addition and leave the rest to the reader. Suppose that f, g and h are three functions from X to R. We want to prove

$$(f + g) + h = f + (g + h).$$

Since both sides are functions from X to R, it suffices to prove that they have the same effect on any element $x \in X$.

$$\begin{aligned} ((f + g) + h)(x) &= (f + g)(x) + h(x) \\ &= (f(x) + g(x)) + h(x) \\ &= f(x) + (g(x) + h(x)) \\ &= f(x) + (g + h)(x) \\ &= (f + (g + h))(x). \end{aligned}$$ □

Here is a very interesting example of this type.

Example 14.8. *Let $X = [0, 1]$ and $R = \mathbb{R}$. Then we are looking at the collection of all functions from X into the reals. In this case there are lots of interesting subrings. For example consider $C[0, 1]$, the set of all continuous functions from $[0, 1]$ into $\mathbb{R}$. Since the sum and product of two continuous functions is continuous, it follows that this is a subring of the set of all functions. Similarly we could look at the space of all differentiable (or twice, thrice, up to infinitely differentiable) functions.*

Definition-Lemma 14.9. *Let R be a ring and let n be a positive integer. $M_n(R)$ denotes the set of all $n \times n$ matrices with entries in R. Given two such matrices $A = (a_{ij})$ and $B = (b_{ij})$, we define $A + B$ as $(a_{ij} + b_{ij})$. The product of A and B is also defined in the usual way. That is the ij entry of AB is the dot product of the ith row of A and the jth column of B.*

With this rule of addition and multiplication $M_n(R)$ becomes a ring, with zero given as the zero matrix (every entry equal to zero) and 1 given as the matrix with ones on the main diagonal and zeroes everywhere else.

Proof. Most of this has already been proved and that which has not, is left as an exercise for the reader. □

Note that is $n = 1$, then $M_1(R)$ is simply a copy of R. To fix ideas, let us consider an easy example.

Example 14.10. *Let $R = \mathbb{Z}_6$ be the ring of integers modulo six and take $n = 2$. Take*

$$A = \begin{pmatrix} 3 & 1 \\ 2 & 4 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 5 \\ 1 & 2 \end{pmatrix}$$

Then

$$AB = \begin{pmatrix} 4 & 5 \\ 0 & 0 \end{pmatrix}.$$

Definition-Lemma 14.11. *Let R be a ring and let x be an indeterminate. The* ***polynomial ring*** *$R[x]$ is defined to be the set of all formal sums*

$$a_n x^n + a_{n-1} x^n + \dots a_1 x + a_0 = \sum a_i x^i$$

where each $a_i \in R$. Given two polynomials

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0 = \sum a_i x^i$$

$$g = b_m x^m + b_{m-1} x^{m-1} + \dots b_1 x + b_0 = \sum b_i x^i$$

in $R[x]$ the sum of f and g, $f + g$, is defined as,

$$f+g = (a_n+b_n)x^n+(a_{n-1}+b_{n-1})x^{n-1}+\dots(a_1+b_1)x+(a_0+b_0) = \sum(a_i+b_i)x^i,$$

(where we have implicitly assumed that $m \leq n$ and we set $b_i = 0$, for $i > m$) and the product as

$$fg = c_{m+n}x^{m+n}+c_{m+n-1}x^{m+n-1}+\dots c_1x^1+c_0 = \sum_i c_i x^i = \sum_i (\sum_j a_j b_{i-j}) x^i.$$

With this rule of addition and multiplication, $R[x]$ becomes a ring, with zero given as the polynomial with zero coefficients and 1 given as the *polynomial whose constant coefficient is one and whose other terms are zero.*

Proof. A long and completely uninformative check. □

Note that a polynomial, determines a function $R \longrightarrow R$ in an obvious way. If one takes R to be the real numbers, then it is well known that a polynomial is determined by the corresponding function. In general, however, this is far from true. For example take $R = \mathbb{Z}_2$ (the smallest ring possible, since a ring must contain at least two elements). Then there are four functions from R to R and there are infinitely many polynomials. Thus two different polynomials will often determine the same function.

Example 14.12. *The final example is a famous and beautiful generalisation of the complex numbers. The complex numbers are obtained by adding a formal number i to the real numbers and decreeing that $i^2 = -1$.*

The quaternions are obtained from the real numbers by adding three new numbers, i, j and k. Thus the set of all quaternions is equal to the set of all formal sums

$$a + bi + cj + dk,$$

where a, b, c and d are real numbers. It is obvious how to define addition,

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a')+(b+b')i+(c+c')j+(d+d')k.$$

Multiplication is a little more complicated. The basic idea is to define how to multiply any two of i, j and k and from there extend by using the associative and distributive laws. Thus we define

$$i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j.$$

In this case, we define the multiplication as,

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k) = (aa' - bb' - cc' - dd')$$
$$+ (ab' + b'a + cd' - dc')i + (ac' + ca' + db' - bd')j + (ad' + da' + bc' - b'c)k.$$

Again it is not so hard to check that this does gives us a group.

If one look at the real numbers, then the numbers ± 1 form a group under multiplication, isomorphic to $\mathbb{Z}_2$. Similarly the complex numbers ± 1, $\pm i$ form a group under multiplication, isomorphic to $\mathbb{Z}_4$. It is in fact not hard to see that the quaternion numbers, ± 1, $\pm i$, $\pm j$ and $\pm k$ form a group of order eight under multiplication (if you like, think of the multiplication rule above as giving generators and relations).