9. Rings

We introduce the main object of study for 103B.

Definition 9.1. *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.

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

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

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

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

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

Example 9.2. *The complex numbers $\mathbb{C}$ are a ring.*

Definition 9.3. *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 9.4. *Let R be a ring and let S be a non-empty subset.*

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

Proof. Similar proof as for groups. □

Example 9.5. *The following tower of subsets*

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

is in fact a tower of subrings. Thus the integers, rational numbers, reals and complex numbers are all rings.

Example 9.6. *Let $\mathbb{Z}_n$ denote the integers modulo n. We already know that this forms a group under addition. It is also the case that multiplication is well-defined so that $\mathbb{Z}_n$ is a ring.*

It is interesting to see what happens in a specific example. Suppose that $n = 6$. In this case $0 = [0]$. 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 9.7. *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).

Proof. This is standard but somewhat tedious to check. $\square$

Note that if $n = 1$ then $M_1(R)$ is simply a copy of R.

To fix ideas, let us consider an easy example of a matrix ring.

Example 9.8. *Let $R = \mathbb{Z}_6$ be the ring of integers modulo 6 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

$$AB = \begin{pmatrix} 3+1 & 15+2 \\ 2+4 & 10+8 \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 0 & 0 \end{pmatrix}.$$

Definition-Lemma 9.9. *Consider the set F of functions from $\mathbb{R}$ to $\mathbb{R}$. We already know how to add to such functions: given f and $g \in F$, define $f+g$ by the rule,*

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

where $x \in \mathbb{R}$ and addition is in $\mathbb{R}$. In words, we add the functions pointwise.

Under addition F becomes a group. There is an obvious way to multiply two functions: define $f \cdot g$ by the rule,

$$(f \cdot g)(x) = f(x) \cdot g(x) \in \mathbb{R},$$

where $x \in \mathbb{R}$ and multiplication is in $\mathbb{R}$. In words we multiply two functions pointwise.

With this rule of addition and multiplication F becomes a ring.

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 $\mathbb{R}$ to $\mathbb{R}$, it suffices to prove that they have the same effect on any real number $x \in \mathbb{R}$.

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

□

Example 9.10. *$n\mathbb{Z}$ is a subring of $\mathbb{Z}$, since the sum and product of two multiples of n is a multiple of n.*

Example 9.11. *If R and S are rings then the Cartesian product is naturally a ring. We have already seen that $R \times S$ is naturally an abelian group under addition. If we define multiplication by the rule:*

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$$

then it is not hard to see that $R \times S$ is a ring.