MSM203a: Polynomials and rings
Chapter 1: Introduction

Richard Kaye

Autumn 2013*

Note: These printed handouts are intended to supplement the material provided in lectures. They are not sufficient on their own.

1 The axiomatic method: numbers

You have already seen various sets of numbers, including the integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$. These are obviously different but have many common features. This course studies the common features of them all. Another aspect of this course is to show how to make new kinds of number, new number systems, and study their properties.

This begs the question, 'what is a number?' You have probably been led to think that a number is a kind of object, and when one looks at such an object it is obvious somehow that it is the right sort of thing to be called a number. So for example, the set $\{0, 1\}$ is not a number. But this view is very limiting, and taking this view will prevent one discovering a whole range of exciting mathematics.

We will take the view that, instead of an object x being either a number or not, it will be viewed in some *context* and that context will tell us the properties of x. We will look at those contexts and properties which make x behave like a number. It will not matter whether x happens to be a banana or the set $\{0, 1\}$ or something else—it is how it behaves that matters.

Another way of saying this is that mathematical objects are not what they are, *but what they do*. The contexts we study will include operations such as add and multiply, so in such contexts x can add to or multiply with another object y. The operations (and the set of objects that are subject to these operations) are key here, not the objects themselves.

We can make this idea more formal and precise, but first we need a piece of set theoretic notation from first year.

Definition 1.1. Suppose X, Y are sets. Then $X \times Y$ denotes the set of pairs of the form (x, y) where x is from X and y is from Y. This is called the *Cartesian Product* of X and Y. A special case is $X \times X$, the set of pairs (x_1, x_2) where both $x_1, x_2 \in X$. The product $X \times X$ is often written X^2.

This generalises: we can form the product $X \times Y \times Z$ of all triples (x, y, z) where $x \in X$, $y \in Y$, $z \in Z$, and we can form $X^3 = X \times X \times X$. And so on to X^4, X^5, etc.

Definition 1.2. Let X be a set. An *operation* on X is a function $f\colon X \to X$. A *binary operation* on X is a function $f\colon X \times X \to X$.

Notice that X is automatically 'closed' under any operation on X so I don't ever have to state this as an 'axiom'.

In examples, a suggested definition of an operation on a set X may not be obviously well-defined, for example because it is not obvious if the set is closed under that operation. We will have to bear this in mind.

*Version 2.1b of 2013-10-04

We will be looking at '*ring-like structures*'. These are nonempty sets X with two binary operations, $+\colon X^2 \to X$ and $\cdot\colon X^2 \to X$ which we think of as being like addition and multiplication. We'll even write them like addition and multiplication, so writing $x+y$ instead of $+(x,y)$ and $x \cdot y$ or xy instead of $\cdot(x,y)$. We will assume the usual rule of precidence, multiplication before addition, so $x + yz$ means $x + (y \cdot z)$. But these operations need not be the familiar addition and multiplication. You may write a ring-like structure as $(X, +, \cdot)$ to emphasise the fact that there are three pieces of information: the set X and the two operations $+, \cdot$. It is more common to write it just as X, but you must remember that specifying the operations $+, \cdot$ is still important.

Example 1.3. Let X be the set of subsets of $\mathbb{N}$. For $x, y \in X$ define $x + y := x \cup y$ and $x \cdot y := x \cap y$. Then X is closed under these operations and this therefore defines a ring-like structure.

The most important ring-like structures are $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with their usual addition and multiplication operations. There are many many other examples. If we are going to study them we should not study one, and then move to the next, and so on, since this would waste a lot of time. But we should as far as possible study all of them simultaneously, concentrating on the ways they are similar or the ways they are different. We can start by listing some of the properties (we will call them *axioms*) that they have.

▶ **AXIOM 1.** Addition is associative, $x + (y + z) = (x + y) + z$ for all x, y, z.

▶ **AXIOM 2.** There is a special element called zero and written 0 such that $x + 0 = 0 + x = x$ for all x.

Proposition 1.4. If a ring-like structure satisfies Axiom 2 then there is only one element 0 satisfying $x + 0 = 0 + x = x$ for all x.

Proof. See lectures.[1] □

▶ **AXIOM 3.** For all x there is an element y such that $x + y = y + x = 0$.

Proposition 1.5. If a ring-like structure satisfies Axioms 1, 2 and 3 then for each x there is only one element y satisfying $x + y = y + x = 0$.

The unique y with $x + y = y + x = 0$ will be written $-x$. Thus this defines a unary operation $x \mapsto -x$ on X. But we may also define a *binary* operation of subtraction for ring-like structures satisfying Axioms 1, 2 and 3 by $x - y := x + (-y)$. (There is no need to prove closure here: this is obvious from closure under $+$.)

▶ **AXIOM 4.** Addition is commutative, $x + y = y + x$ for all x, y.

▶ **AXIOM 5.** Multiplication is associative, $x(yz) = (xy)z$ for all x, y, z.

▶ **AXIOM 6.** Multiplication is distributive over addition, $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all x, y, z.

Definition 1.6. A *ring* is a ring-like structure satisfying axioms 1, 2, 3, 4, 5, and 6.

You might think we could add more axioms, but we will stop here and look at the effect of other axioms later. Stopping here has the advantage that any theorems we can prove about rings will be very general: they only need these six axioms to work.

Example 1.7. The set of integers $\mathbb{Z}$ with the usual addition and multiplication is a ring.

Example 1.8. The set of rationals $\mathbb{Q}$ with the usual addition and multiplication is a ring.

Example 1.9. The set of reals $\mathbb{R}$ with the usual addition and multiplication is a ring.

[1] In future, for any theorem, proposition, lemma, example, etc. stated in these notes that needs a proof, but the proof is omitted here, the proof will be given in lectures. You may be asked to reproduce some of these proofs in the exam.

Example 1.10. The set of complex numbers $\mathbb{C}$ with the usual addition and multiplication is a ring.

Example 1.11. The set $M_2(\mathbb{R})$ of 2×2 matrices with real entries with the usual addition and multiplication of matrices is a ring.

Example 1.12. The set $R = \{0\}$ with addition and multiplication defined by $0+0 = 0 \cdot 0 = 0$ is a ring, called the *zero ring*.

Example 1.13. The set $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ of integers modulo n with the usual addition and multiplication modulo n is a ring.[2]

Example 1.14. The set of *Gaussian Integers* $\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\}$ with addition and multiplication defined as for complex numbers is a ring. (In this case it is important to check closure under the addition and multiplication operations as well as the axioms, because subsets of $\mathbb{C}$ may not be closed under addition and multiplication as defined on $\mathbb{C}$.)

Example 1.15. The set $\mathbb{Z}[\sqrt{2}] = \{x + y\sqrt{2} : x, y \in \mathbb{Z}\}$ with addition and multiplication defined as for real numbers is a ring. (Again, it is important to check closure.)

We will have a lot to say about the last three examples and others like it throughout this module.

Definition 1.16. Let R be a ring and S a subset of R containing the 0 of R and closed under $+, -, \cdot$. then S is a *subring* of R. Using the operations from R, it satisfies all of the axioms of being a ring in its own right.

Note that we had to include $-$ as one of our operations here. This was to make sure the subring satisfies Axiom 3.

Not every ring-like structure is a ring. In fact there are many more non-rings than rings: being a ring is somehow rather special.

Exercise 1.17. Let X be the set of subsets of $\mathbb{N}$ with $x + y := x \cup y$ and $x \cdot y := x \cap y$. Then X is not a ring.

Exercise 1.18. The set $\mathbb{N}$ with usual addition and multiplication is not a ring.

These (and hundreds of other examples) should convince you that if you want to define a ring it is not sufficient to say what the set is and define addition and multiplication. You also need to prove that the set is closed under these operations and that the axioms are all true.

Finally, don't forget that the addition and multiplication are just names and do not necessarily mean the usual operations.

Exercise 1.19. The set $\mathbb{R}^+$ of positive real numbers with addition defined by $x + y := xy$ and multiplication defined by $x \cdot y := x^{\log y}$ is a ring, where 'log' means to base e, i.e. natural logarithm.[3] (When you do this, be careful you distinguish between 'the usual addition' and the addition in the ring-like structure, and also 'the usual multiplication' and the multiplication in the ring-like structure, and understand what is being asked here.)

Exercise 1.20. The set $\mathbb{R}^+$ of positive real numbers with addition defined by $x + y := xy$ and multiplication defined by $x \cdot y := x^y$ is not a ring.

2 Consequences of the axioms

A lot of basic properties of numbers in rings follow from our six basic axioms. One highlight is that $(-x)(-y) = xy$ holds for all x, y in a ring. (Finally you will understand the reason why the product of two negative numbers is positive!) All of this will be done in lectures.

[2] Unfortunately, in some places this ring is called $\mathbb{Z}_n$, and in other places $\mathbb{Z}_n$ is something different. The notation $\mathbb{Z}/n\mathbb{Z}$ is the only unambiguous one I know for this ring.

[3] I'd use 'ln()' but I cannot pronnounce it without feeling very foolish indeed!

3 Other axioms: integral domains and fields

Looking ahead slightly, we can add other axioms to our list. The axioms in this section are *not* in general true of all rings but describe 'special' rings.

▶ **AXIOM 7.** Multiplication is commutative, $xy = yx$ for all x, y.

Definition 3.1. A ring satisfying Axiom 7 is called a *commutative ring*.

Exercise 3.2. The ring $\mathbb{Z}$ with usual addition and multiplication is a commutative ring.

Exercise 3.3. The ring $M_2(\mathbb{Z})$ of 2×2 matrices over $\mathbb{Z}$ is not commutative.

▶ **AXIOM 8.** There is an element 1 such that $1x = x1 = x$ for all x.

Definition 3.4. A ring satisfying Axiom 8 is called a *ring with one*.

We reserve the word 'unit' for later, to mean something quite different. So don't ever talk about 'ring with a unit' (however posh it might sound).

Proposition 3.5. In a ring with one the element 1 satisfying $1x = x1 = x$ for all x is unique. If the ring has more than one element then $1 \neq 0$.

Example 3.6. The ring of integers $\mathbb{Z}$ with usual addition is commutative with one.

Exercise 3.7. The set of even integers $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ with usual addition and multiplication is a ring. It is commutative but doesn't have one.

The last part of the last exercise contains a major trap that you must not fall into. Remember that 1 is the *name* for 'a one' in a ring R. It may not be the number usually called 1. (Think of Example 1.19 which is a commutative ring with one, where the element 1 is actually e.)

To prove $2\mathbb{Z}$ does not have one, suppose $y \in 2\mathbb{Z}$ is a 'one' in $2\mathbb{Z}$. Then $xy = yx = x$ for all $x \in 2\mathbb{Z}$. But $y = 2n$ for some $n \in \mathbb{Z}$ and multiplication is the usual one in the integers, so $x(2n) = (2n)x = x$ for all $x \in 2\mathbb{Z}$. In particular this needs to hold for $x = 2 \in 2\mathbb{Z}$. So $4n = 2(2n) = (2n)2 = 2$, so $n = 1/2$ which is impossible as n was supposed to be an integer.

Exercise 3.8. The set of even integers $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ with usual addition and with multiplication defined by $x \cdot y := xy/2$ is a commutative ring with one. (Here $\cdot$ is the multiplication I have defined and xy is the usual multiplication.) You should check closure as well as the other axioms.

Example 3.9. The zero ring $\{0\}$ is a commutative ring with one.

We will spend quite a lot of time later on talking about commutative rings with one.

Other additional features of some rings that doesn't come for free from our previous axioms concerns multiplication. In a 'bad' ring R it may be that two nonzero numbers multiply together to give zero.

Example 3.10. In the ring $\mathbb{Z}/6\mathbb{Z}$ of integers modulo 6, we have $[2] \cdot [3] = [0]$.

Definition 3.11. In a ring R, a number x is a *zero divisor* if it is nonzero and there is some nonzero y such that one or both of xy, yx is 0.

▶ **AXIOM 9.** There are no zero divisors: $xy = 0$ implies $x = 0$ or $y = 0$ for all x, y.

Proposition 3.12. Let R be a ring. Then R has no zero divisors if and only if the left and right cancellation laws hold:

$$\text{if } x \neq 0 \text{ and } xy = xz \text{ then } y = z \tag{1}$$

$$\text{if } x \neq 0 \text{ and } yx = zx \text{ then } y = z \tag{2}$$

Definition 3.13. A *integral domain* is a ring R which is commutative with one and which has no zero divisors.

Example 3.14. The ring $\mathbb{Z}$ with usual addition and multiplication is an integral domain.

Example 3.15. The ring of integers modulo 6 is not an integral domain.

▶ **AXIOM 10.** $0 \neq 1$.

▶ **AXIOM 11.** For all nonzero x there is a y such that $xy = yx = 1$.

Proposition 3.16. Given x in a ring with one, if there is y such that $xy = yx = 1$ this y is unique.

When y exists such that $xy = yx = 1$ we write it as x^{-1} or $1/x$.

Definition 3.17. A *field* is a commutative ring R with one that satisfies axioms 10 and 11.

I didn't include the 'no zero divisors' axiom becase it is not needed.

Proposition 3.18. Any field is an integral domain.

Example 3.19. The ring of integers $\mathbb{Z}$ with usual addition and multiplication is an integral domain but not a field.

Example 3.20. The ring of integers modulo 5 is a field.

We will have a lot more to say about fields later too.

4 Polynomials

A major part of this module is about polynomials. You have seen polynomials before but may not have seen a definition. In keeping with the rigorous approach here, we need to define them properly.

This section will contain the briefest of introductions to polynomials. They will be used throughout the module, for examples and exercises, and these notes will summarise their properties.

You may be surprised by the role that polynomials play in this course. You should stop thinking about polynomials as functions and think of them as *numbers*. For any ring R we will define the set of polynomials $R[X]$ over R, and the most important fact will be that $R[X]$ is a ring in its own right. In other words, its elements, the polynomials, behave just as numbers behave (so they *are* numbers). Moreover there is a copy of the original R in $R[X]$. Thus $R[X]$ defines a 'bigger' set of numbers extending R.

Now, more slowly, and more rigorously, we give the definitions.

Definition 4.1. Let R be a ring. A polynomial with coefficients from R is a sequence

$$(r_0, r_1, \ldots, r_n, 0, 0, \ldots)$$

of elements $r_i \in R$, such that all but finitely many of these elements are zero.

That's strange and doesn't (yet) agree with our previous intuition about polynomials. It will help if we write them slightly differently.

Definition 4.2. Let R be a ring and X a letter. We let $R[X]$ be the set of polynomials with coefficients from R where we write the polynomial

$$(r_0, r_1, \ldots, r_n, 0, 0, \ldots)$$

in the special way as

$$r_0 + r_1 X + \cdots + r_n X^n.$$

We usually write the polynomial $r_0 + r_1 X + \cdots + r_n X^n$ as $p(X)$ for some letter p.

Definition 4.3. We define addition in $R[X]$ as follows. Let $r(X) = r_0 + r_1X + \cdots + r_nX^n$ and $s(X) = s_0 + s_1X + \cdots + s_kX^k$ be polynomials in $R[X]$. That is, they are sequences

$$r(X) = (r_0, r_1, \ldots, r_n, 0, 0, \ldots)$$

and

$$s(X) = (s_0, s_1, \ldots, s_k, 0, 0, \ldots).$$

Then we define $r(X) + s(X)$ to be the polynomial $t(X)$ defined by

$$t(X) = (r_0 + s_0, r_1 + s_1, \ldots).$$

Notice that as all but finitely many r_i are zero, all but finitely many s_i are zero, and $0+0 = 0$ it follows that all but finitely many $r_i + s_i$ are zero.

Definition 4.4. We define multiplication in $R[X]$ as follows. Let $r(X) = r_0 + r_1X + \cdots + r_nX^n$ and $s(X) = s_0 + s_1X + \cdots + s_kX^k$ be polynomials in $R[X]$. That is, they are sequences

$$r(X) = (r_0, r_1, \ldots)$$

and

$$s(X) = (s_0, s_1, \ldots).$$

Then we define $r(X) \cdot s(X)$ to be the polynomial t(X) defined by

$$t(X) = (r_0s_0, r_1s_0 + r_0s_1, t_2, t_3, \ldots, t_m, \ldots)$$

where

$$t_m = \sum_{i=0}^{m} r_i s_{m-i}$$

for each m. Notice that as $r_i = 0$ for $i > n$ and $s_j = 0$ for $j > k$ it follows that $t_m = \sum_{i=0}^{m} r_i s_{m-i} = 0$ for $m > n + k$ since if $m > n + k$ and $0 \leqslant i \leqslant m$ then either $i > n$ or else $i \leqslant n$ and $m - i > k$ so one of r_i, s_{m-i} is zero. Hence $r_i s_{m-i} = 0$ for all such i, so $t_m = 0$. So $t(X) \in R[X]$.

Theorem 4.5. If R is a ring then $R[X]$ is also a ring.

Definition 4.6. If R is a ring with one, and $p(X) \in R[X]$ we say $p(X)$ is *monic* if its leading coefficient is 1, i.e. if $p(X) = 1 \cdot X^k + p_{k-1}X^{k-1} + \cdots + p_1X + p_0$ for some k.

Definition 4.7. If R is a ring and $p(X) \in R[X]$ is non-zero, then the *degree of* $p(X)$, $\deg p(X)$ is the unique n such that $p(X) = (p_0, p_1, p_2, \ldots, p_n, 0, 0, \ldots)$ and $p_n \neq 0$.

In the special case when $p(X) = (0, 0, \ldots)$ is the zero of $R[X]$ we define the degree of $p(X)$ to be -1.[4]

Note that this makes R essentially the 'same as' the set of polynomials $p(X) \in R[X]$ such that $\deg p(X) \leqslant 0$. In other words $R[X]$ contains a 'copy' of R, the set of polynomials $r(X) = r_0$. That is, R is *isomorphic to a subring of* $R[X]$.

Theorem 4.8. If R is a commutative ring with one then $R[X]$ is also a commutative ring with one.

Theorem 4.9. If R is an integral domain then $R[X]$ is also an integral domain.

However it is *not* true that if R is a field then $R[X]$ is a field. For example, in $\mathbb{R}[X]$, the 'one' is $1 = 1 + 0X + 0X^2 + \cdots$. And X (an abbreviation for $0 + 1X$) is not the 0. But there is no polynomial $p(X)$ such that $p(X) \cdot X = 1$, for if $p(X) = p_0 + p_1X + \cdots + p_nX^n$ were such a polynomial then $p_n \neq 0$ for some $n > 0$ else $p(X) = p_0 \in \mathbb{R}$ and $p(X) \cdot X = p_0X \neq 1$. But if $p_n \neq 0$ with $n > 0$ then $p(X) \cdot X = p_0X + \cdots + p_nX^{n+1}$ and this polynomial cannot equal 1.

A lot of this module is concerned with how to recover from this difficulty: in particular how to make $R[X]$ into a field. Of course this will involve either adding new elements or merging elements together or defining new addition and multiplication operations. In other words there needs to be other ways of making 'new rings' from old ones. The two key methods are: (a) quotient rings; and (b) the field of fractions. We will study these both in due course.

[4]Other people say that the degree of 0 to be $-\infty$ or just 'not defined' so you need to take care here.