

# Abstract Algebra: An Outline

William Traves

June 22, 1996

## 1 An Invitation to Begin

Of necessity these notes cannot contain a discussion but I will try to keep the tone light and anticipate your questions. As well, these notes are not intended as a substitute for the lectures given by Clifton Cunningham. Indeed, I propose to take a radically different approach. In class you had to build the edifice of mathematics from the ground up. But now that the foundations have been laid, we can discuss the material from a sophisticated standpoint. Even so, these notes are being written because a textbook for the course is not readily available. The primary difficulty is that we lack a reference for the precise statements of our definitions and theorems. These can be found in the appendix. Also, I refer the reader to the many references listed at the end of this paper.

One of my fondest memories of my undergraduate studies is of the evenings that I spent discussing mathematics with my mentor, Tony Geramita. In my mind I recall the comfortable armchairs in his living room and a warm fire keeping away the winter's cold. Of course, I have romanticised this scene greatly and the reality was likely far more prosaic. But I recall this story to emphasize that mathematics is best learned by discussing our difficulties and insights with our friends. Also, it is very important to be comfortable and relaxed; then one's mind is free to concentrate on the essential details of our discussion. I won't ask you to imagine yourself in Tony's living room. For one thing it is summer and too hot for a fire. But as I write these notes I imagine that I am sitting with a friend on my roofdeck, watching the evening sky appear and talking quietly about some of the things that we have learned. It might help you to keep a similar picture in your mind as you read on. But now, please, let us begin.

## 2 Algebraic Structures: Rings and Things

Much of our course was concerned with studying rings like  $\mathbf{Z}$  (the integers) or  $\mathbf{Q}$  (the rationals) or polynomial rings over them (such as  $\mathbf{Q}[x]$ ). These are among the most elementary rings and this is no accident. It is here that we first encounter the notions of abstract algebra in a concrete setting. For most people  $\mathbf{Z}$  is the first ring that they meet:  $\mathbf{Z}$  is a set with two binary operations, addition and multiplication, that satisfy various properties individually and some distributive properties in conjunction (see the appendix for precise definitions). The rationals,  $\mathbf{Q}$ , are among the first fields that we meet: each nonzero element of  $\mathbf{Q}$  is a unit (i.e. has a multiplicative inverse). The ring of matrices over any other ring (for instance  $M_{2 \times 2}(\mathbf{Z})$ ) provide an example of a ring which is not an integral domain: there are nonzero matrices which multiply to give the zero matrix (we even asked you to find some on your first assignment). It is important that an abstract ring is just a set with two operations and these operations need not correspond to our conventional notions of addition and multiplication (if we define  $\times$  on  $\mathbf{Z}$  by  $a \times b = 0$  for all  $a, b \in \mathbf{Z}$  then  $(\mathbf{Z}, +, \times)$  is a ring (without unit)). These simple examples provide a first glimpse of some complicated behaviour of general rings; this is apparent when we look at the ideal structure

of these rings.

Most of the rings that we will consider will have a unity element (i.e. 1) but in general we don't require this of our rings. The reason is that if we drop the requirement for the existence of 1 then there is a nice relation between subrings and ideals. Recall that a subring  $S$  is just a set which is contained in a ring  $R$  and which is a ring in its own right under the additive and multiplicative structure induced from  $R$ . So, for instance,  $\mathbf{Q}$  has lots of subrings. An ideal is just a subring  $S$  which is closed under the multiplicative action of the ring  $R$  (i.e.  $rs \in S$  for each  $r \in R$  and  $s \in S$ ). In general this is precisely the kind of subobject that we need to define the quotient,  $\frac{R}{S}$ . We'll talk more about this later but for now, note that there are very few ideals of  $\mathbf{Q}$ : just  $(0)$  and  $\mathbf{Q}$  itself. On the other hand,  $\mathbf{Z}$  has many ideals. It turns out that  $\mathbf{Z}$  is a principal ideal domain: it is an integral domain in which every ideal can be generated by a single element. The ideals of  $\mathbf{Z}$  look like  $(n) = \{kn : k \in \mathbf{Z}\}$  where  $n$  is any integer. The ideal structure of the ring  $\mathbf{Z}[X]$  is not so nice though: the ideal consisting of all polynomials with even constant term is not principally generated (but what elements do generate this ideal?). So we must be careful in trying to infer properties about  $R[X]$  from properties about  $R$ .

One nice property that does extend from  $R$  to  $R[X]$  is the unique factorization property. This property generalizes what is known as the fundamental theorem of arithmetic: every nonzero, noninvertible integer factors uniquely as a product of primes (up to multiplication by a unit and up to the position of the factors). To generalize this property to an arbitrary ring we need to have a good notion of primality. While we might have been taught something different in elementary school, a prime integer can be defined as a nonzero, noninvertible integer  $p$  such that for any integers  $r$  and  $s$ :  $p|rs \Rightarrow p|r$  or  $p|s$  (here  $a|b$  means  $a$  divides  $b$ ). Replacing integer by element in the above definition gives us a definition of a prime element of a ring. What we all learned as our first definition of prime number corresponds to the notion of an irreducible element of a ring  $R$ : a nonzero, nonunit element  $q \in R$  is irreducible if  $q = rs \Rightarrow$  one of  $r$  or  $s$  is a unit. In  $\mathbf{Z}$  the notions of prime and irreducible coincide but this is not true in general (I'll leave it to you to find an example where they are not the same). In any case, the unique factorization property holds for a ring  $R$  (and we say that  $R$  is a UFD) if any nonzero, nonunit element of  $R$  can be expressed uniquely as a product of irreducibles (up to order of the factors and multiplication by a unit).

This leads naturally to the related notions of Euclidean Domains, greatest common divisors and the division algorithm. I'll talk about these things in the next section. But before we move on, I'd like to tell you a little about how ideals were discovered. Of course, we have seen that ideals can be used to develop the quotient ring structure. This provides a typical technique to try to solve certain diophantine equations: equations like  $x^2 - 3y^2 + 7z^2 = 17$  with solutions in the integers. The idea is to reduce the equation *mod*  $p$  for each prime  $p$  (i.e. reduce the coefficients *mod*  $p$ ) and then try to solve the equation in the ring  $\frac{\mathbf{Z}}{(p\mathbf{Z})} \cong \mathbf{F}_p$ . If one has complete information about these

cases then often one can lift this information back to  $\mathbf{Z}$  to tell us about the integer solutions to the equation (this is called the Hasse Principle and is one of the highlights of number theory). Another interesting thing about ideals is that they generalize numbers. While certain rings (like  $\mathbf{Z}[\sqrt{-5}]$ ) may not be unique factorization domains, they still might have a unique factorization of ideals. This relates to a famous false attempt to solve Fermat's Last Theorem (just recently proven by Andrew Wiles, who built upon hundreds of years of work in algebra). That proof failed precisely because certain rings did not have unique factorization. Kummer attempted to correct this problem by showing that, in certain rings, ideals have a unique factorization property. This leads to a notion of a prime ideal. We will return to this when we talk about commutative algebra and algebraic geometry but for now we make an interesting definition of a prime ideal: an ideal  $P$  is prime if for any two ideals  $I$  and  $J$  of  $R$  we have  $IJ \subset P \Rightarrow I \subset P$  or  $J \subset P$ . Since, in the integers,  $(n) \subset (m) \iff m|n$  we see that this definition of prime ideal corresponds to our notion of prime element. It is an interesting exercise to show that this notion of prime ideal gives the same thing as our other characterizations of prime ideals.

### 3 How to Divide in $\mathbf{Z}$

The division algorithm gives a way of computing the greatest common denominator of any pair of integers. Indeed, reversing the steps of the algorithm gives a representation of  $(f, g)$ , the *gcd* of  $f$  and  $g$ , as a linear combination of  $f$  and  $g$  with coefficients in  $\mathbf{Z}$ . So any *gcd* of  $f$  and  $g$  is of the form  $af + bg$  with  $a, b \in \mathbf{Z}$ . Indeed, an argument involving the well-ordering of the integers shows that the positive *gcd* of  $f$  and  $g$  (which is what we mean when we write  $(f, g)$ ) is the least positive element of the set  $\{af + bg : a, b \in \mathbf{Z}\}$ . Of course in the assignments we asked you to show that the *gcd* is unique up to multiplication by a unit and that the *gcd* operation is associative (so that we can define the *gcd* of any finite collection of integers). Things get interesting when we try to generalize this notion of greatest common divisor to arbitrary rings.

First note that what we are using in proving the above results is the division algorithm and this depends on having a good notion of size (an ordering on the elements of the ring; for example, absolute value in  $\mathbf{Z}$  or degree in  $\mathbf{Z}[X]$ ). Domains with this kind of ordering are called Euclidean Domains (see the appendix for a precise definition). In such rings we can define a division algorithm and use this to get information about *gcds*. The *gcd* then turns out to be unique up to multiplication by a unit and we generally single out a particular kind of *gcd* to be denoted by  $(f, g)$  (for example, the positive one in  $\mathbf{Z}$  and the monic one in  $\mathbf{Q}[X]$ ).

Some rings do not have the unique factorization property; for example,  $\mathbf{Z}[\sqrt{-5}]$  (check this as an exercise). Here we cannot say (as we might in a UFD) that the *gcd* of two elements is the product of all the irreducibles that appear in both the factorization of  $f$  and of  $g$  (counted with their multiplicities). Instead we generalize the properties of *gcds* in  $\mathbf{Z}$  to get an abstract definition of a *gcd*:

an element  $c \in R$  is a *gcd* of  $f, g \in R$ , denoted  $c = (f, g)$ , if  $c|f$ ,  $c|g$  and if any  $d \in R$  divides both  $f$  and  $g$  then  $d|c$ . Many times on the assignments we asked you to prove results about *gcds*. With this abstract definition of *gcd* all you need to do to show that an element  $e \in R$  is equal to  $(f, g)$  is to show that the properties above hold for  $e$  (in place of  $c$ ) and that  $e$  is of the proper form (for example,  $e$  is positive if  $R = \mathbf{Z}$  or monic if  $R = \mathbf{Q}[X]$ ). This approach was emphasized in the solutions to the problem sets.

It is no accident that we use the notation  $(f, g)$  for both the *gcd* of  $f$  and  $g$  and the ideal generated by  $f$  and  $g$ . In fact, if we are in a PID (principal ideal domain) then these two notions coincide:  $d = \text{gcd}(f, g)$  if and only if  $(d) = (f, g)$ .

Given the ease of defining the greatest common divisor in a UFD it is desirable to have a nice way to check whether a given ring is a UFD. Unfortunately, I don't know of any such method. But one set of implications is known and is quite important:  $R$  is a Euclidean Domain  $\Rightarrow R$  is a PID  $\Rightarrow R$  is a UFD.

It is often important to be able to tell whether a certain element of a ring is irreducible or not. In general this is a very hard problem but in certain rings (like  $\mathbf{Q}[X]$ ) we have powerful tools to help us. For instance, Gauss's lemma tells us that any *monic* polynomial with integer coefficients is reducible in  $\mathbf{Q}[X]$  if and only if it is reducible in  $\mathbf{Z}[X]$ . Often it is then possible to apply Eisenstein's test to the polynomial (though sometimes we must modify the polynomial  $P(X)$  and consider instead the equivalent problem for the polynomial  $Q(X) = P(X+n)$  ( $n \in \mathbf{Z}$ )).

Sometimes it is possible to use the so-called rational root test to check for irreducibility of a polynomial in  $\mathbf{Z}[X]$ . If we can assume that if our polynomial  $P(X) = \sum_{i=0}^{i=n} a_i X^i$  ( $a_n \neq 0$ ) is reducible then it has a linear factor (for instance if  $\deg P(X) \leq 3$ ) then it suffices to show that  $P(\frac{r}{s}) \neq 0$  for all integers  $r|a_0$  and  $s|a_n$ .

There is another method in  $\mathbf{Z}[X]$  that never fails though it takes more work. Suppose our polynomial is  $P(X) = \sum_{i=0}^{i=n} a_i X^i$  ( $a_n \neq 0$ ). If  $P(X) = F(X)G(X)$  then w.l.o.g.  $\deg F(X) \leq \frac{n}{2}$ . Take  $N$  to be the integer part of  $\frac{n}{2}$  and find the value of  $P(X)$  at  $N$  integer points  $\{a_1, \dots, a_N\}$  (it helps if you can find values that are prime). Then  $F(a_i)|P(a_i)$  and  $F(a_i) \in \mathbf{Z}$  so there are a limited number of possible values for  $F(a_i)$ . Since  $N$  points determine a polynomial of degree at most  $n$  uniquely (use Lagrange's interpolation theorem) we see that there are a limited (though possibly large) number of possibilities for  $F(X)$ . For each of these we test whether  $F(X)|P(X)$  (an efficient method is to choose another point  $b \in \mathbf{Z}$  and check whether  $F(b)|P(b)$ ; if this does not hold then  $F(X)$  does not divide  $P(X)$  but if this holds for many choices of  $b$  then one should check  $F(X)|P(X)$  directly). Note that one need not check all possible values of  $F(X)$ : symmetry among the possible values ensures that we need only check one of  $F(X)$  and  $-F(X)$ .

All of this is fairly involved but things get even more complicated in polynomial rings of more than one variable. There one wishes to devise a division algorithm that works for more than a pair of polynomials: for instance, what

should we mean by the remainder of  $4X^3Y^2+5Y^3+21$  upon division by  $2X^2Y-4$  and  $3y-2$ ? This relates to the ideal structure of such rings and is an active area of current research. For more information on the division algorithm in polynomial rings and the related notion of Groebner bases, see [3] (this is an excellent book, written at an accessible level, which also details some cool ways to use algebraic techniques in the design of automobiles and robots).

## 4 Abstract Algebra

In the last section we discussed arithmetic in  $\mathbf{Z}[X]$  and  $\mathbf{Q}[X]$ . Abstract Algebra abstracts this discussion in two ways: we will be concerned with arithmetic in more general rings and we will concern ourselves with the manipulation not only of elements of the rings but of the rings themselves. This will become clear when we discuss quotient rings. One of the principles of Abstract Algebra is that in order to understand an algebraic object, it is important to understand the maps between these objects. What is a map between two rings?

A map between two rings is just a function  $f : R \rightarrow S$  that preserves both the additive and multiplicative structure of the rings: that is,  $f(a \oplus_R b) = f(a) \oplus_S f(b)$  and  $f(a \odot_R b) = f(a) \odot_S f(b)$  for all  $a, b \in R$ . This definition is sufficient if we are considering non-unitary rings but if our rings have 1 then we also require that  $f(1)=1$  (note that  $f(0) = 0$  automatically). A map between two rings that respects the ring structures is called a ring homomorphism. A ring homomorphism which is 1-1 is called injective and a ring homomorphism which is onto is called surjective. A ring homomorphism which is both injective and surjective is called an isomorphism and the two rings are said to be isomorphic. Isomorphism is a precise way of saying that two rings are *equal as rings*; we denote this relation by  $R \cong S$ .

The map  $f : \mathbf{Z}[X] \rightarrow \mathbf{Z}[\sqrt{-5}]$  which is the identity on the integers and sends  $X$  to  $\sqrt{-5}$  is an example of a homomorphism which is surjective but not injective ( $f(x^2 + 5) = 0$ ). The map  $\iota : \mathbf{Z}[X] \rightarrow \mathbf{Q}[X]$  is a homomorphism which is injective but not surjective. Whenever we have an ideal  $I$  of a ring  $R$  we can consider the equivalence relation on elements of  $R$  which says that two elements are equivalent if they differ by an element of  $I$ . Denote the equivalence class of  $a \in R$  by  $[a]$ . Then we check that the operations on  $R$  induce operations on the set of equivalence classes of elements of  $R$ . When doing this we need to ensure that these operations are well-defined: for example, we need to check that the operation  $[a] + [b] = [a + b]$  does not depend on our choice of representatives for the equivalence classes  $[a]$  and  $[b]$ . (This is not as difficult as it sounds. If  $[a] = [r]$  then  $a - r \in I$  and if  $[b] = [s]$  then  $b - s \in I$ . But then  $[a + b] = [r + s]$  since  $(a + b) - (r + s) = (a - r) + (b - s) \in I$ .) Once all this is done we have the ring of equivalence classes of  $R \bmod I$ , denoted  $\frac{R}{I}$ . We also have the ring homomorphism  $\phi : R \rightarrow \frac{R}{I}$  defined by  $\phi(a) = [a]$ . Note that  $\phi$  is surjective: the image of  $\phi$  (often denoted  $\phi(R)$ ) is all of its range,  $\frac{R}{I}$ .

Just as was the case with vector spaces, both the image and the the kernel (or nullity) of the map are important. The kernel of  $\phi : R \rightarrow S$  is the set of

elements of  $R$  that are sent to 0 under  $\phi$  (various violent language is used to describe the kernel; for instance, elements of the kernel are *killed* or *annihilated* (I have even heard *assassinated!*) by the map  $\phi$ ). Note that the kernel of the natural map  $\phi : R \rightarrow \frac{R}{I}$  is just the ideal  $I$ . In fact this phenomenon is true for ring homomorphisms in general: the kernel of a ring homomorphism is an ideal of the domain ring.

We are now in a position to discuss the decomposition of ring homomorphisms and the isomorphism theorems. The first ring isomorphism theorem says that if  $\phi : R \rightarrow S$  is a ring homomorphism then  $Im(\phi) \cong \frac{R}{Ker(\phi)}$  (that is, the image of  $R$  is isomorphic to the quotient ring  $\frac{R}{Ker(\phi)}$ ). In fact, any ring homomorphism factors as a composition of a surjective and injective homomorphisms:  $f : R \rightarrow S$  factors as  $f = \iota \circ \phi$  where  $\phi : R \rightarrow \frac{R}{Ker(f)}$  is the natural map and  $\iota : \frac{R}{Ker(f)} \rightarrow S$  is map given by the identification of  $\frac{R}{Ker(f)}$  with  $Im(f)$ . The second and third isomorphism theorems are also important (see the appendix for precise statements).

## 5 Geometry

It might seem strange to be talking about geometry in an algebra course but mathematics is a unity and the best work in one area often illuminates things in another. I'll explain all this in a bit, but first we need to discuss prime and maximal ideals.

Prime ideals are those ideals  $P \subset R$  such that  $\frac{R}{P}$  is an integral domain (ring having no zero divisors). Equivalently, prime ideals are those rings such that if  $ab \in P$  then one of  $a$  or  $b$  is in  $P$ . We can order the ideals in a ring by inclusion:  $I < J \iff I \subset J$ . The largest ideals with respect to this ordering are called maximal ideals (they exist by Zorn's lemma - a useful lemma from set theory; you can take this on faith if you wish). You should prove to yourself that maximal ideals are prime and that if  $m$  is a maximal ideal then  $\frac{R}{m}$  is a field. Both  $(X)$  and  $(p)$  ( $p$  a prime number) are prime ideals of  $\mathbf{Z}[X]$ ; the ideal  $(X, p)$  is a maximal ideal in  $\mathbf{Z}[X]$ .

Now I'd like to explain the correspondence between ideals in  $\mathbf{C}[X_1, \dots, X_n]$  and geometric objects (curves, surfaces, etcetera) in  $\mathbf{C}^n$ . Any ideal  $I$  in  $\mathbf{C}[X_1, \dots, X_n]$  is generated by a finite set of polynomials (that this generating set is finite is the content of the famous Hilbert Basis Theorem - see David Eisenbud's excellent book [4] for the statement and many proofs of this theorem). To this ideal we can associate the set of common zeros of these generators, a set we denote by  $\mathbf{V}(I) \subset \mathbf{C}^n$ . I leave it to you to check that this set is well-defined (it is independent of our choice of generators for  $I$ ). Conversely, given a set of points  $X \subset \mathbf{C}^n$  we define the ideal  $\mathbf{I}(X)$  of polynomials in  $\mathbf{C}[X_1, \dots, X_n]$  which vanish on  $X$ . Again, you should check for yourself that this is an ideal. There is a nice correspondence between these two operations: for any ideal  $I$ :  $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ . Here, we have used  $\sqrt{I}$  to denote the radical of  $I$ : the ideal of polynomials, some power of which is in the ideal  $I$ . If ideals correspond to these

zero sets of polynomials, what do prime and maximal ideals correspond to?

Prime ideals correspond to particularly nice zero sets. A zero set  $X$  is reducible if it is the nontrivial union of two other zero sets (for example,  $\mathbf{V}(X_1 X_2) = \mathbf{V}(X_1) \cup \mathbf{V}(X_2)$  = the union of the  $X_1$  and  $X_2$ -axes in  $\mathbf{C}^2$ ). A zero set is called irreducible if it is not reducible. Prime ideals correspond to irreducible zero sets. Maximal ideals correspond to the simplest possible irreducible zero sets, points (to get an idea of why this is true, note that the two operations,  $\mathbf{I}$  and  $\mathbf{V}$ , are inclusion reversing).

Of course, I have only spoken about ideals in  $\mathbf{C}[X_1, \dots, X_n]$ . A similar theory can be worked out for the polynomial rings  $\mathbf{Z}[X_1, \dots, X_n]$  and  $\mathbf{Q}[X_1, \dots, X_n]$ . More generally, we can define these notions for an arbitrary ring (see the discussion of  $\text{Spec } R$  in Eisenbud's book [4]).

This discussion has wandered a bit far from the content of the course but I think that it is important for you to get a feeling for the relationship of abstract algebra to algebraic geometry. This interplay between geometric intuition and algebraic computation has been one of the most successful (and beautiful!) facets of modern mathematics.

## 6 Fields and Espionage

This is certainly the sexiest chapter in these notes. We will talk a bit about Field theory. The most important mathematician who worked in field theory (Evariste Galois) was a revolutionary who was killed in a duel and many of its modern practioners currently work for various spy agencies around the world (yes, even here in Canada!). For more on the remarkable life (and death) of Galois, see Infeld's entertaining novel [6] (the author's own life was quite remarkable too).

We have already mentioned the definition of fields (rings with unity where every nonzero element is invertible). There are two types of fields and they are classified by their characteristic. We often denote fields by letters such as  $K$  or  $L$ . Take the natural ring homomorphism  $\phi : \mathbf{Z} \rightarrow \mathbf{K}$  sending 1 to 1. The kernel of this homomorphism is a prime ideal of  $\mathbf{Z}$  (since the image of  $\phi$  is a subring of  $\mathbf{K}$  and hence is a domain). So  $\ker(\phi) = (0)$  or  $(p)$  (for some prime number  $p$ ). This generator of the kernel is called the characteristic. An example of a characteristic zero field is  $\mathbf{Q}$  while any of the finite fields have prime characteristic. As an exercise you should produce an example of a field of prime characteristic which is not finite.

One of the most elementary (though very subtle) ideas about fields is the notion of a field extension. If  $K \subset L$  are fields then we say that  $L$  is an extension field of  $K$  (and  $K$  is a subfield of  $L$ ). The classic example is  $\mathbf{Q} \subset \mathbf{R}$  and we will return to this in a moment. But first, what is the smallest field containing  $\mathbf{Q}$  and  $\sqrt{2}$ ? Clearly this field  $\mathbf{Q}(\sqrt{2})$  contains all elements of the form  $a + b\sqrt{2}$  where  $a$  and  $b$  are rational numbers and then all inverses of such elements and then all polynomial combinations in these elements and then all inverses of such elements ... whew! In fact, all elements of the form  $a + b\sqrt{2}$  are elements of the quotient ring  $\frac{\mathbf{Q}[X]}{(X^2-2)}$ . Since  $(X^2-2)$  is a maximal ideal in  $\mathbf{Q}[X]$ , these elements

already form a field! So  $\mathbf{Q}(\sqrt{2}) \cong \frac{\mathbf{Q}[X]}{(X^2-2)}$ . A further example is furnished by  $\mathbf{C} \cong \mathbf{R}(\sqrt{-1}) \cong \frac{\mathbf{R}[X]}{(X^2+1)}$  (this last example is quite interesting: adding the solution to  $X^2 + 1$  to  $\mathbf{R}$  ensures that **every** polynomial (in one variable) over the resulting ring ( $\mathbf{C}$ ) has a solution in that ring; this property is summed up by saying that  $\mathbf{C}$  is algebraically closed - this is the content of the Fundamental Theorem of Algebra). In general to find the field  $\mathbf{Q}(\alpha)$  ( $\alpha \in \mathbf{C}$ , say) we find the minimal degree monic polynomial with coefficients in  $\mathbf{Q}$  which has  $\alpha$  as a root; call this polynomial  $P_\alpha$ . Then  $\mathbf{Q}(\alpha) \cong \frac{\mathbf{Q}[X]}{(P_\alpha)}$ . You can generalize this to arbitrary field extensions on your own (consider the extension  $K(\alpha, \beta)$  of  $K$ ).

This seems fine for finite extensions of a field (where  $\dim_K L < \infty$ ). But what about the field extension  $\mathbf{Q} \subset \mathbf{R}$ ? Presumably we could write  $\mathbf{R} = \mathbf{Q}(\alpha_1, \alpha_2, \dots)$  and try to make some sense out of this but we won't do that here. In fact,  $\mathbf{R}$  is the completion of  $\mathbf{Q}$  in its standard Euclidean metric. That is,  $\mathbf{R}$  is the set of equivalence classes of Cauchy sequences (see any reasonable Calculus textbook for the definition of a Cauchy sequence; for example, see [8]) of elements of  $\mathbf{Q}$ . We add and multiply Cauchy sequences componentwise and this gives our standard ring structure on  $\mathbf{R}$ .

The notion of a Cauchy sequence depends on the metric that we are using (the distance function). In the above example, the metric (usually denoted by  $|\cdot|$ ) was the standard Euclidean metric on  $\mathbf{Q}$ . But we can use a more arithmetic metric on  $\mathbf{Q}$ : let  $p$  be a prime number and for each integer  $m$  set  $\gamma_p(m)$  to be the number of occurrences of  $p$  in the prime factorization of  $m$ ; then define  $|\cdot|_p : \mathbf{Q} \rightarrow \mathbf{R}$  by  $|\frac{m}{n}|_p = p^{-(\gamma_p(m) - \gamma_p(n))}$ . This also gives a metric on  $\mathbf{Q}$ . Two integers are close together in this metric if their difference is divisible by a high power of  $p$ . This metric is very useful in number theoretic problems. The completion of  $\mathbf{Q}$  with respect to this metric is called  $\mathbf{Q}_p$ , the  $p$ -adic numbers. The truly adventurous student might show that this field is isomorphic to the Field of Laurent series over the finite field  $\mathbf{F}_p$  (see a textbook on Complex Analysis for the definition of Laurent series; for example, see [7]). Then one can play with the addition and multiplication of elements of this completion (which is quite an interesting exercise).

Now I want to summarize the basic facts about finite fields. We have already seen that they all have prime characteristic. If  $L$  is a finite field of characteristic  $p$  we have  $\mathbf{F}_p \subset L$ . Then the number of elements of  $L$  is  $p^{[L:\mathbf{F}_p]} = p^{\dim_{\mathbf{F}_p}(L)}$  and so  $L$  has  $p^n$  elements. So each finite field has size  $p^n$  for some prime number  $p$  and some nonnegative integer  $n$ . It turns out that these fields are given by the quotient  $\frac{\mathbf{F}_p[X]}{(f)}$  where  $f$  is a monic polynomial irreducible over  $\mathbf{F}_p$  of degree  $n$ . Also, any field of size  $p^n$  is isomorphic to any other! So finite fields are uniquely determined by their size.

Okay, so where is all this exciting spy stuff? It has to do with coding theory. If one wants to send secret messages then one often encodes them in a secret code (which the enemy will try to break). This coding scheme often uses the arithmetic of finite fields (as do most computations involving computers). The secret code has more recently been replaced by public-key cryptography but the

mathematical ideas are still related to much of what we have been studying here. A more serious problem for code senders is the presence of a noisy channel. For instance, if I am sending information across a telephone line (using a modem, say) and the line is defective and introduces garbage characters into my message (changes the value of sent characters) then how can the receiver tell that the message has been corrupted? How can the receiver fix the message? These are the problems that motivated error-detecting and error-correcting codes. These codes safeguard information by encoding the message in a redundant manner which uses finite field arithmetic as a check for message corruption. These ideas are important in the design of high speed modems, bar-code scanners and internet protocols. For more on coding theory, the reader could consult [5].

Finally a few words about Galois' beautiful theorem are in order. To state it we must first know what a group is. This is just a set with an associative binary operation which has a null element and an inverse for each element. For example,  $(\mathbf{Z}, +)$  is a group. Also, the permutations on  $n$  symbols (with the operation being composition of permutations) is a group. Note that the group operation need not be commutative. Given a finite field extension  $K \subset L$ , what are the intermediate extensions  $F$  (that is, fields  $F$  such that  $K \subset F \subset L$ )? To describe the answer we must define the group of automorphisms of  $L$  fixing  $K$ : this is the set of isomorphisms from  $L$  to itself such that each element of  $K$  is a fixed point of the map. These maps form a group under composition and we denote it  $|Gal(L/K)|$ . Then, under some further technical assumptions on the extension  $K \subset L$ , we have that the map

$$\Phi : (\text{intermediate subfields of } K \subset L) \rightarrow (\text{subgroups of } Gal(L/K))$$

given by  $\Phi(F) = Gal(L/F)$  is a 1-1 inclusion reversing map. So the intermediate fields of this extension are classified by the subgroups of  $Gal(L/K)$ ! This amazing relationship of field theory to group theory forms the backbone of much of modern algebra. In particular, it relates to the factorization of polynomials and ruler-and-compass questions posed by the ancients. A complete account of this beautiful theorem can be found in Allenby's book [1] or Michael Artin's textbook [2].

## 7 Conclusion and Farewell

In conclusion I would like to emphasize that mathematics should not be compartmentalized into disjoint fields: algebra relates to geometry, to topology and finally to the calculus. In turn, each of these subjects informs our view of algebraic systems. Many of the exciting mathematical theories (Galois theory,  $p$ -adic analysis and algebraic geometry) span more than one area of mathematics.

I appreciate this opportunity to discuss abstract algebra with you. It is an honour to be allowed to speak about the achievements of the great mathematicians of the past. I hope that some of the things that we have seen in these notes will encourage you to take a deeper look at what we have studied. Good luck and farewell!

## 8 Appendix: Precise Statements

In this appendix we list the precise statements of all relevant definitions and collect the statements of important theorems that we treated in the course. The order of the statements reflects my own sense of the logical development of the theory.

A **ring** is a set  $R$  with two binary operations, addition (+) and multiplication ( $\times$ ) which satisfy the following properties:

(1) There is a null element for addition:  $\exists 0 \in R$  such that for each  $r \in R$ ,  $r + 0 = 0 + r = r$ .

(2) For each element  $r \in R$  there exists an element  $-r \in R$  such that  $r + (-r) = (-r) + r = 0$ .

(3) Addition is associative: for any three elements  $r, s, t \in R$  we have  $(r + s) + t = r + (s + t)$ .

(4) Multiplication is associative: for any three elements  $r, s, t \in R$  we have  $(r \times s) \times t = r \times (s \times t)$ .

(5) Multiplication distributes over addition and vice-versa: for any three elements  $r, s, t \in R$  we have  $r \times (s + t) = (r \times s) + (r \times t)$  and  $(r + s) \times t = (r \times t) + (s \times t)$ .

Often we write omit the multiplication symbol; this is standard in integer multiplication and should cause no confusion. There are many different kinds of rings. The most common are **unitary rings**: these rings possess an identity element for multiplication ( $\exists 1 \in R$  such that for each  $r \in R$ ,  $1 \times r = r \times 1 = r$ ).

Elements  $r$  in a unitary ring  $R$  which have multiplicative inverses (that is,  $\exists s \in R$  such that  $rs = 1$ ) are called **units**. Rings in which every nonzero element is a unit are called **fields**. A nonzero element  $r \in R$  is called a **zero divisor** if there is another nonzero element  $s \in R$  such that  $rs = 0$ . Rings with no zero divisors are called **domains** (or **integral domains**).

A **subring**  $S$  of a ring  $R$  is a subset  $S \subset R$  such that the binary operations on  $R$  restrict to binary operations on  $S$  and under these induced operations,  $S$  is a ring. An **ideal** is a subring  $I$  which is closed under the multiplicative action of  $R$ : for each  $r \in R$  and  $a \in I$  we have  $ra \in I$ . The ideal generated by elements  $\{a_1, \dots, a_n\} \subset R$  is denoted by  $(a_1, \dots, a_n)$  and is defined to be  $\{\sum_{i=1}^n r_i a_i : r_i \in R\}$ .

One element  $r \in R$  is said to **divide** another element  $s \in R$ , written  $r|s$ , if there exists a third element  $t \in R$  such that  $s = rt$ . An element  $r \in R$  is said to be **prime** if whenever  $r|(st)$  we have  $r|s$  or  $r|t$ . An element  $r \in R$  is said to be **irreducible** if whenever  $r = st$  then one of  $s$  or  $t$  is a unit. Note that in a domain, prime elements are irreducible but the converse is not always true. If  $r = ut$  where  $u$  is a unit then  $r$  and  $t$  are said to be **associates**. If  $d|r$  and  $d|s$  then  $d$  is said to be a **common divisor of  $r$  and  $s$** .

Let  $c$  be a common divisor of  $r$  and  $s$  such that for every other common divisor  $d$  of  $r$  and  $s$ ,  $d|c$ , then we call  $c$  a **greatest common divisor of  $r$  and  $s$** . Note that a greatest common divisor ( $gcd$ ) is unique up to associates. We often denote a special greatest common divisor by  $(r, s)$ : in the integers this is the positive  $gcd$ ; in a polynomial ring it is the monic  $gcd$ . Two elements  $r$  and  $s$  are said to be **relatively prime** (or **coprime**) if  $(r, s) = 1$ . The **division**

**algorithm for  $\mathbf{Z}$**  says that if  $a, b \in \mathbf{Z}$  with  $b \neq 0$  then there exist unique integers  $m$  and  $r$  such that  $a = mb + r$  with  $0 \leq r < |b|$ . Applying this (see the assignments) gives that for two integers  $a$  and  $b$  (not both zero),  $(a, b) = ta + sb$  for some integers  $t$  and  $s$ . In fact, in the integers,  $(a, b)$  turns out to be the least positive value of this form  $(ta + sb)$ . Associated to these ideas is the **Euclidean Algorithm** for computing the *gcd* of two nonzero integers  $a$  and  $b$ . At step one use the division algorithm to find integers  $m_1$  and  $r_1$  such that  $a = m_1b + r_1$  where  $0 \leq r_1 < |b|$ . Then at step two use the division algorithm to find integers  $m_2$  and  $r_2$  such that  $b = m_2r_1 + r_2$  where  $0 \leq r_2 < |r_1|$ . At step three find integers  $m_3$  and  $r_3$  such that  $r_1 = m_3r_2 + r_3$  where  $0 \leq r_3 < |r_2|$ . Continue in this manner until  $r_n = 0$ . Then  $(a, b) = r_{n-1}$ .

The integers also have a **unique factorization property**. Let  $a$  be a nonzero integer. Then either  $a$  is a unit or  $a$  can be written as the product of a unit and finitely many positive primes. Further, if  $a = up_1p_2 \dots p_n = vq_1q_2 \dots q_m$  where  $u$  and  $v$  are units and  $p_1, \dots, p_n, q_1, \dots, q_m$  are positive primes then  $u = v$ ,  $m = n$  and the  $p_i$  and the  $q_j$  can be paired off in such a manner that paired primes are equal.

We shall assume that the student is familiar with the notion of a polynomial. The polynomials in one variable  $X$ , with coefficients in the ring  $R$ , are denoted  $R[X]$ . One should check that the units in  $R[X]$  are just the units in  $R$ . Polynomials which are not irreducible elements of  $R[X]$  are called **reducible**. The *gcd* of the coefficients of a polynomial is called the **content** of that polynomial and the polynomial is called **primitive** if its content is 1. A polynomial is called **monic** if its leading coefficient is 1. These notions are used to prove **Gauss's Lemma**: if  $F \in \mathbf{Q}[X]$  is a monic polynomial with integer coefficients then  $F$  is reducible in  $\mathbf{Q}[X]$  if and only if  $F$  is reducible in  $\mathbf{Z}[X]$ . Furthermore, if  $F = fg$  in  $\mathbf{Q}[X]$  then  $F = pq$  in  $\mathbf{Z}[X]$  where  $\deg f = \deg p$  and  $\deg g = \deg q$ .

**Eisenstein's Test** is a useful way to conclude that a polynomial is irreducible. Let  $F = \sum_{i=0}^n a_i X^i$  be a polynomial in  $\mathbf{Z}[X]$  such that there is a prime integer  $p$  with (1)  $p|a_0, p|a_1, \dots, p|a_{n-1}, p \nmid a_n$  and (2)  $p^2 \nmid a_0$ , then  $F$  is irreducible in  $\mathbf{Q}[X]$ . Note that the converse to Eisenstein's Test does not hold.

There is an analogue of the unique factorization theorem for the integers for the two polynomial rings  $\mathbf{Z}[X]$  and  $\mathbf{Q}[X]$  (just make the obvious modifications in the above statement for  $\mathbf{Z}$  - change prime to irreducible polynomial). Similarly there is a division algorithm in  $\mathbf{Q}[X]$ : if  $f, g \in \mathbf{Q}[X]$  with  $g \neq 0$  then there exist  $m, r \in \mathbf{Q}[X]$  such that  $f = mg + r$  and either  $r = 0$  or  $r \neq 0$  and  $\deg r < \deg g$ . This gives a Euclidean algorithm for  $\mathbf{Q}[X]$ .

A polynomial  $f(X) \in R[X]$  is said to have a **root** at  $a$  if  $f(a) = 0$ . The **remainder theorem** says that if  $a$  is a root of  $f$ , then  $(x - a)|f$ . The **rational root test** says that if  $\frac{r}{s}$  is a rational root of the polynomial  $a_0 + a_1X + \dots + a_nX^n \in \mathbf{Z}[X]$  where  $(r, s) = 1$  then  $r|a_0$  and  $s|a_n$ . This helps in determining whether cubic polynomials are irreducible. The **Fundamental Theorem of Algebra** describes the factorization of polynomials in  $\mathbf{C}[X]$ : every nonconstant polynomial over  $\mathbf{C}$  has a root in  $\mathbf{C}$ . It follows from the remainder theorem that every nonconstant polynomial in  $\mathbf{C}[X]$  can be expressed as a product of linear terms.

In using **Kronecker's test for irreducibility** (see section 3) we need to use **Lagrange's Interpolation Theorem**. This states that if  $u_1, \dots, u_{n+1}$  are distinct rationals and  $v_1, \dots, v_{n+1}$  are rationals (not necessarily distinct) then there is exactly one polynomial  $f \in \mathbf{Q}[X]$  such that (1)  $\deg f \leq n$  and (2)  $f(u_i) = v_i$  for each  $i$ . The actual polynomial is:

$$f(X) = \sum_{i=1}^{n+1} v_i \frac{(X - u_1) \dots (X - u_{i-1})(X - u_{i+1}) \dots (X - u_{n+1})}{(u_i - u_1) \dots (u_i - u_{i-1})(u_i - u_{i+1}) \dots (u_i - u_{n+1})}.$$

A **binary operation** on a set  $A$  is a map  $f : A \times A \rightarrow A$ . This is distinct from the notion of a **binary relation** on a set  $A$ , which is a subset  $R$  of  $A \times A$ . If  $(a, b) \in R$  then we write  $aRb$ . The relation  $R$  is: **reflexive**, if  $xRx$  for all  $x \in A$ ; **symmetric**, if  $xRy \Rightarrow yRx$  for all  $x, y \in A$ ; **transitive**, if  $xRy$  and  $yRz \Rightarrow xRz$  for all  $x, y, z \in A$ . If  $R$  is reflexive transitive and symmetric then we call  $R$  an **equivalence relation**. The classic example of an equivalence relation is the relation of equivalence *mod*  $n$  on the set of integers. A **partition** of a set is a collection of nonempty sets which are pairwise disjoint and whose union is the whole set. Each equivalence relation gives rise to a partition of our set  $A$ . Also, each partition gives rise to an equivalence relation on  $A$ . The subsets in the partition are called **equivalence classes** of the associated relation. Given a ring  $S$  and a relation  $R$  on  $S$  we often can check that the operations on  $S$  devolve to operations on the equivalence classes of  $R$ . This gives us a new ring whose set is the equivalence classes of  $R$  and whose operations are induced from the operations on  $S$ . The best example of this is the quotient ring (see below).

Using these ideas we can obtain some results in number theory. For instance, **Fermat's Little Theorem** says that if  $p$  is a positive prime integer and  $n$  is a positive integer then  $p | (n^p - n)$  (that is,  $n^p \equiv n \pmod{p}$ ). For a positive integer  $m$ , let  $\phi(m)$  be the number of integers between 1 and  $m$  which are relatively prime to  $m$ . This function is called Euler's  **$\phi$ -function** or the **totient** function. Then we have: let  $a$  and  $m$  be positive integers which are relatively prime, then  $a^{\phi(m)} \equiv 1 \pmod{m}$ . Finally, we have **Wilson's Theorem**: let  $p$  be a positive prime; then  $(p - 1)! \equiv -1 \pmod{p}$ .

We now deal with types of rings which relate to unique factorization. A **Euclidean valuation** on a ring  $R$  is a map  $\delta : R \setminus \{0\} \rightarrow \mathbf{Z}^+ \cup \{0\}$  such that: (1) for all nonzero  $a, b \in R$ ,  $\delta(a) \leq \delta(ab)$  and (2) if  $a, b \in R$  with  $b \neq 0$  then there exist  $m, r \in R$  such that  $a = mb + r$  and either  $r = 0$  or  $r \neq 0$  and  $\delta(r) < \delta(b)$ . A domain with a Euclidean valuation is called a **Euclidean Domain (ED)**. There are a number of examples of Euclidean valuations. The absolute value on the integers is one such function. The degree function on  $\mathbf{Q}[X]$  is another. A somewhat different kind of function is given by the map  $N : \mathbf{Z}[\sqrt{-5}] \rightarrow \mathbf{Z}$  defined as  $N(a + b\sqrt{d}) = |a^2 + db^2|$ . This is called the **norm** map. Note that  $N(\alpha) = 0 \iff \alpha = 0$  and  $N(\alpha\beta) = N(\alpha)N(\beta)$ .

Domains which have the unique factorization property are called **UFDs**. Domains in which every ideal is principally generated (generated by a single element) are called **Principal Ideal Domains (PIDs)**. We have the theorem that:  $\text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD}$ .

Given a domain  $R$  we can form a new **ring of fractions**  $S = \{\frac{r}{s} : r, s \in R, s \neq 0\}$ . We say that two fractions  $\frac{r}{s}$  and  $\frac{a}{b}$  are equal if  $br - as = 0$ . Given a field the intersection of all of its subfields is also a field (the smallest subfield) and is called the **prime subfield**. If  $K$  has characteristic 0 then this prime subfield is  $\mathbf{Q}$  and if  $K$  has characteristic  $p$  then this prime subfield is  $\mathbf{F}_p$  (see section 6 for the definition of the **characteristic** of a field).

Given an ideal  $I$  of a ring  $R$  we can form the equivalence relation of equality *mod*  $I$ :  $a \equiv b \iff a - b \in I$ . The equivalence classes of this relation have a ring operation induced from the ring operation on  $R$  (see my comments about factor rings in section 4). This new ring is called a **factor ring** and is denoted  $\frac{R}{I}$ .

An ideal  $P$  of a ring  $R$  is **prime** if  $ab \in P \implies a \in P$  or  $b \in P$  for all  $a, b \in R$ . Equivalently, an ideal  $P$  is prime if and only if  $\frac{R}{P}$  is an integral domain. An ideal  $m$  of  $R$  is **maximal** if there are no larger proper ideals in  $R$ : that is, if  $I$  is an ideal of  $R$  and  $m \subset I \subset R$  then  $I = m$  or  $I = R$ . Note that  $m$  is maximal if and only if  $\frac{R}{m}$  is a field.

The concepts of **ring homomorphism** and **ring isomorphism** are treated in section 4 of these notes. We have three important **ring isomorphism theorems**. The first ring isomorphism theorem is treated in section 4 of the notes. For the second ring isomorphism theorem we need the concept of the sum of an ideal and a subring. Let  $A$  be an ideal and  $B$  be a subring of the ring  $R$ . Define  $A + B$  to be the subset  $\{a + b : a \in A, b \in B\}$  of  $R$  and check that  $A + B$  is a subring of  $R$ ,  $A$  is an ideal of  $A + B$  and  $A \cap B$  is an ideal of  $B$ . Then we have that  $\frac{A+B}{A} \cong \frac{B}{A \cap B}$  ( $\cong$  denotes ring isomorphism). The third ring isomorphism theorem says that if  $I \subset J$  are ideals of a ring  $R$  then  $\frac{J}{I} = \{j + I : j \in J\}$  is an ideal in  $\frac{R}{I}$  and  $\frac{R/I}{J/I} \cong \frac{R}{J}$ .

These ideas are used in the construction of **finite fields** and field extensions. For more on this, see section 6 of the notes.

## References

- [1] R.B.J.T. Allenby. *Rings, Fields and Groups*. Second Edition. Edward Arnold, London: 1991.
- [2] Michael Artin. *Algebra*. Prentice-Hall, Englewood Cliffs, NJ: 1991.
- [3] Cox, Little and O'Shea. *Ideals, Varieties and Algorithms*. Springer, New York: 1992.
- [4] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, New York: 1995.
- [5] Raymond Hill. *A First Course in Coding Theory*. Clarendon Press, Oxford: 1990.
- [6] Leopold Infeld. *Whom the Gods Love, the Story of Evariste Galois*. Whittlesay House, New York: 1948.

- [7] Marsden, J. E. and Hoffman, M. J. *Basic Complex Analysis*. Second Edition. W. H. Freeman and Company, New York: 1987.
- [8] Michael Spivak. *Calculus*. Third Edition. Publish or Perish, Inc., Houston: 1994.