Module MA3411: Commentary
Polynomial Rings
Michaelmas Term 2009

D. R. Wilkins

Contents

C Polynomial Rings

C-1 Rings of Polynomials and Formal Power Series

Let R be a unital commutative ring.

Let us denote by $\hat{R}$ the set of all infinite sequences $(r_0, r_1, r_2, \ldots)$ indexed by the set of non-negative integers, where $r_j \in R$ for $j = 0, 1, 2, \ldots$. For each element $\mathbf{r}$ of $\hat{R}$, and for each non-negative integer j, let us denote by $\mathbf{r}_{[j]}$ the component of $\mathbf{r}$ indexed by j. Thus if $\mathbf{r} = (r_0, r_1, r_2, \ldots)$, where $r_j \in R$ for each non-negative integer j, then $\mathbf{r}_{[j]} = r_j$ for $j = 0, 1, 2, \ldots$.

Given elements $\mathbf{a}$, and $\mathbf{b}$ of $\hat{R}$, let $\mathbf{a} + \mathbf{b}$ denote the element of $\hat{R}$ which satisfies $(\mathbf{a} + \mathbf{b})_{[j]} = \mathbf{a}_{[j]} + \mathbf{b}_{[j]}$ for all non-negative integers j. Thus if $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ and $\mathbf{b} = (b_0, b_1, b_2, \ldots)$, then

$$\mathbf{a} + \mathbf{b} = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots).$$

We obtain in this way an operation of addition defined on the set $\hat{R}$. This operation of addition is commutative and associative. Also $\mathbf{a} + \mathbf{0} = \mathbf{a}$ and $\mathbf{a} + (-\mathbf{a}) = \mathbf{0}$ for all $\mathbf{a} \in \hat{R}$, where

$$\mathbf{0} = (0, 0, 0, \ldots) \quad \text{and} \quad -(a_0, a_1, a_2, \ldots) = (-a_0, -a_2, -a_3, \ldots).$$

Thus the set $\hat{R}$ is an Abelian group with respect to the operation of addition.

We now introduce a multiplication operation on $\hat{R}$ with the intention of giving $\hat{R}$ the structure of a ring. We could do this by defining the product of the infinite sequences $(a_0, a_1, a_2, \ldots)$ and $(b_0, b_1, b_2, \ldots)$ to be the infinite sequence $(a_0 b_0, a_1 b_1, a_2 b_2, \ldots)$. This is possible, and the resulting operations of addition and subtraction satisfy the ring axioms. But there are other possibilities for the multiplication operation on $\hat{R}$, and we choose to give $\hat{R}$ a multiplication operation whose definition is motivated by the procedures for multiplying polynomials and power series. Specifically, we define the product $\mathbf{a} \times \mathbf{b}$ of elements $\mathbf{a}$ and $\mathbf{b}$ of $\hat{R}$ so that

$$(\mathbf{a} \times \mathbf{b})_{[n]} = \sum_{\substack{j,k \geq 0 \\ j+k=n}} \mathbf{a}_{[j]} \mathbf{b}_{[k]} = \sum_{j=0}^{n} \mathbf{a}_{[j]} \mathbf{b}_{[n-j]}$$

for all non-negative integers n, so that

$$(a_0, a_1, a_2, \ldots) \times (b_0, b_1, b_2, \ldots) = (a_0 b_0,\ a_0 b_1 + a_1 b_0,\ a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots).$$

We proceed to show that $\hat{R}$, with these operations of addition and multiplication, is a unital commutative ring.

Now the ring R is commutative, and therefore

$$(\mathbf{a} \times \mathbf{b})_{[n]} = \sum_{j=0}^{n} \mathbf{a}_{[j]} \mathbf{b}_{[n-j]} = \sum_{k=0}^{n} \mathbf{a}_{[n-k]} \mathbf{b}_{[k]} = \sum_{k=0}^{n} \mathbf{b}_{[k]} \mathbf{a}_{[n-k]}$$

for each non-negative integer n. It follows that $\mathbf{a} \times \mathbf{b} = \mathbf{b} \times \mathbf{a}$ for all $\mathbf{a}, \mathbf{b} \in \hat{R}$.

The operations of addition and multiplication we have defined on $\hat{R}$ satisfy the Distributive Law. Indeed let $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c}$ be elements of $\hat{R}$. Then

$$\begin{aligned}
(\mathbf{a} \times (\mathbf{b} + \mathbf{c}))_{[n]} &= \sum_{j=0}^{n} \mathbf{a}_{[j]} (\mathbf{b} + \mathbf{c})_{[n-j]} = \sum_{j=0}^{n} \mathbf{a}_{[j]} (\mathbf{b}_{[n-j]} + \mathbf{c}_{[n-j]}) \\
&= \sum_{j=0}^{n} \mathbf{a}_{[j]} \mathbf{b}_{[n-j]} + \sum_{j=0}^{n} \mathbf{a}_{[j]} \mathbf{c}_{[n-j]} = (\mathbf{a} \times \mathbf{b})_{[n]} + (\mathbf{a} \times \mathbf{c})_{[n]} \\
&= (\mathbf{a} \times \mathbf{b} + \mathbf{a} \times \mathbf{c})_{[n]}
\end{aligned}$$

for all non-negative integers n. Thus $\mathbf{a} \times (\mathbf{b} + \mathbf{c}) = \mathbf{a} \times \mathbf{b} + \mathbf{a} \times \mathbf{c}$. Similarly $(\mathbf{a} + \mathbf{b}) \times \mathbf{c} = \mathbf{a} \times \mathbf{c} + \mathbf{b} \times \mathbf{c}$. (This identity can be deduced from the previous one either by means of a calculation analogous to the previous one, or else by making use of the fact that the multiplication operation on $\hat{R}$ is commutative.) We have now verified that the algebraic operations on $\hat{R}$ satisfy the Distributive Law.

Let $\mathbf{e} \in \hat{R}$ be defined such that $\mathbf{e}_{[0]} = 1_R$ and $\mathbf{e}_{[j]} = 0_R$ when $j > 0$, where 0_R and 1_R denote the zero element and the multiplicative identity element of the unital commutative ring R. Then $\mathbf{e} \times \mathbf{a} = \mathbf{a} = \mathbf{a} \times \mathbf{e}$ for all $\mathbf{a} \in \hat{R}$.

In order to complete the verification that $\hat{R}$ is a unital commutative ring, it now only remains to show that the multiplication operation defined on $\hat{R}$ is associative.

Let $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c}$ be elements of $\hat{R}$, We show by direct calculation that $(\mathbf{a} \times \mathbf{b}) \times \mathbf{c} = \mathbf{a} \times (\mathbf{b} \times \mathbf{c})$. Now

$$\begin{aligned}
((\mathbf{a} \times \mathbf{b}) \times \mathbf{c})_{[n]} &= \sum_{m=0}^{n} (\mathbf{a} \times \mathbf{b})_{[m]} \mathbf{c}_{[n-m]} \\
&= \sum_{m=0}^{n} \sum_{j=0}^{m} (\mathbf{a}_{[j]} \mathbf{b}_{[m-j]}) \mathbf{c}_{[n-m]} \\
&= \sum_{m=0}^{n} \sum_{j=0}^{m} \mathbf{a}_{[j]} (\mathbf{b}_{[m-j]} \mathbf{c}_{[n-m]}) \\
&= \sum_{\substack{(j,m) \in \mathbb{Z}^2 \\ 0 \leq j \leq m \leq n}} \mathbf{a}_{[j]} (\mathbf{b}_{[m-j]} \mathbf{c}_{[n-m]})
\end{aligned}$$

$$\begin{aligned}
&= \sum_{j=0}^{n}\sum_{m=j}^{n} \mathbf{a}_{[j]}(\mathbf{b}_{[m-j]}\mathbf{c}_{[n-m]}) \\
&= \sum_{j=0}^{n}\sum_{k=0}^{n-j} \mathbf{a}_{[j]}(\mathbf{b}_{[k]}\mathbf{c}_{[n-j-k]}) \\
&= \sum_{j=0}^{n} \mathbf{a}_{[j]}(\mathbf{b}\times\mathbf{c})_{[n-j]} \\
&= (\mathbf{a}\times(\mathbf{b}\times\mathbf{c}))_{[n]}
\end{aligned}$$

for all non-negative integers n. (The indices k and m of summation employed in the above calculation are related by the equation $m = j + k$.)

Alternatively one could establish the associativity of multiplication on $\hat{R}$ by verifying that

$$((\mathbf{a}\times\mathbf{b})\times\mathbf{c})_{[n]} = \sum_{\substack{(j,k,l)\in\mathbb{Z}^2\\ j+k+l=n}} (\mathbf{a}_{[j]}\mathbf{b}_{[k]})\mathbf{c}_{[l]} = \sum_{\substack{(j,k,l)\in\mathbb{Z}^2\\ j+k+l=n}} \mathbf{a}_{[j]}(\mathbf{b}_{[k]}\mathbf{c}_{[l]}) = (\mathbf{a}\times(\mathbf{b}\times\mathbf{c}))_{[n]}.$$

We have now established that $\hat{R}$, with the operations of addition and multiplication defined above, is a unital commutative ring.

Let $\mathbf{x}$ be the element of $\hat{R}$ defined such that $\mathbf{x}_{[1]} = 1_R$ and $\mathbf{x}_{[j]} = 0_R$ for all non-negative integers j satisfying $j \neq 1$, so that

$$\mathbf{x} = (0_R, 1_R, 0_R, 0_R, 0_R, \ldots).$$

Then

$$(\mathbf{x}\times\mathbf{a})_{[0]} = 0_R \quad \text{and} \quad (\mathbf{x}\times\mathbf{a})_{[j+1]} = \mathbf{a}_{[j]}$$

for all non-negative integers j. A straightforward proof by induction on n establishes that

$$\mathbf{x}^n_{[j]} = \begin{cases} 1_R & \text{if } j = n; \\ 0_R & \text{if } j \neq n. \end{cases}$$

for all positive integers n. Moreover this formula is valid for all non-negative integers n, provided that we define $\mathbf{x}^0 = \mathbf{e}$, where $\mathbf{e}$ denotes the identity element $(1_R, 0_R, 0_R, \ldots)$ of $\hat{R}$.

Now let n be a non-negative integer, let $\mathbf{a}$ be an element of $\hat{R}$. Suppose that $\mathbf{a}_{[j]} = 0_R$ for all integers j satisfying $j > n$, so that

$$\mathbf{a} = (a_0, a_1, a_2, \ldots, a_n, 0_R, 0_R, 0_R, \ldots),$$

where $a_j = \mathbf{a}_{[j]}$ for $j = 0, 1, 2 \ldots, n$. Then

$$\mathbf{a} = \sum_{j=0}^{n} a_j\mathbf{x}^j = a_0\mathbf{e} + a_1\mathbf{x} + a_2\mathbf{x}^2 + \cdots + a_n\mathbf{x}^n.$$

Let $\hat{R}_0$ denote the subset of $\hat{R}$ consisting of those elements of $\hat{R}$ with at most finitely many non-zero coefficients. Thus an element $\mathbf{a}$ of $\hat{R}$ belongs to $\hat{R}_0$ if and only if the set of non-negative integers j for which $\mathbf{a}_{[j]} \neq 0_R$ is finite. Now $\mathbf{0} \in \hat{R}_0$, where $\mathbf{0} = (0_R, 0_R, 0_R, \ldots)$, $\mathbf{e} \in \hat{R}_0$, where $\mathbf{e} = (1_R, 0_R, 0_R, \ldots)$ and $\mathbf{x} \in \hat{R}_0$, where $\mathbf{e} = (0_R, 1_R, 0_R, \ldots)$. Also $-\mathbf{a} \in \hat{R}_0$, $\mathbf{a} + \mathbf{b} \in \hat{R}_0$ and $\mathbf{ab} \in \hat{R}_0$ for all $\mathbf{a}, \mathbf{b} \in \hat{R}_0$. Therefore $\hat{R}_0$ is a unital subring of $\hat{R}$ which contains $\mathbf{x}$.

We can regard the ring $\hat{R}_0$ as the ring of polynomials in a single indeterminate with coefficients in the ring R. Indeed every element of $\hat{R}_0$ may be represented as a polynomial expression of the form

$$a_0\mathbf{e} + a_1\mathbf{x} + a_2\mathbf{x}^2 + \cdots + a_n\mathbf{x}^n.$$

Conversely, every such polynomial expression determines a corresponding element of the ring $\hat{R}_0$. The operations of addition and multiplication on $\hat{R}_0$ which $\hat{R}_0$ inherits from the ring $\hat{R}$ correspond to the standard operations used to add and to multiply polynomials. Thus every polynomial with coefficients in the ring R determines a corresponding element of the ring $\hat{R}_0$, and, conversely, every element of the ring $\hat{R}_0$ may be represented as a polynomial with coefficients on the ring R.

We know that the operations of addition and multiplication on $\hat{R}_0$ satisfy the ring axioms, because we have verified that $\hat{R}_0$ is a subring of the larger ring $\hat{R}$. It follows immediately from this that the ring $R[x]$ of polynomials in an indeterminate x with coefficients in a unital commutative ring R is itself a unital commutative ring. Indeed we can *define* $R[x]$ to be the ring $\hat{R}_0$: this gives us a formal construction of the polynomial ring.

Moreover we note that the ring $R[x]$ of polynomials with coefficients in a unital commutative ring R may be embedded in a larger ring $R[[x]]$. This larger ring corresponds to the ring $\hat{R}$ of infinite sequences $(r_0, r_1, r_2, \ldots)$ studied above, where $r_j \in R$ for $j = 0, 1, 2, \ldots$. Let $\mathbf{a}$ be an element of $\hat{R}$, and let $a_j = \mathbf{a}_{[j]}$ for all non-negative integers j. Then $\mathbf{a}$ may be represented as a *formal power series* of the form

$$\sum_{j=0}^{\infty} a_j\mathbf{x}^j.$$

An expression of this form should be regarded as merely a convenient notation for denoting elements of the ring $\hat{R}$, enabling us to regard elements of $\hat{R}$ as *formal power series* with coefficients in the ring R. Considerations of convergence and divergence are totally irrelevant in this context. This notation representing elements of $\hat{R}$ as formal power series respects and emphasizes the fact that each element $\mathbf{a}$ of $\hat{R}$ determines and is determined by an infinite

sequence $a_0, a_1, a_2, \ldots$ of elements of the ring R. The customary procedures for adding and multiplying together power series correspond to the operations of addition and multiplication defined on the ring $\hat{R}$. Moreover this power series notation is consistent with the representation of elements of the subring $\hat{R}_0$ as polynomials of the form $f(\mathbf{x})$ whose coefficients belong to the ring R.

We see therefore that to any unital commutative ring R we can associate a ring $R[[x]]$. The elements of this ring $R[[x]]$ are in one-to-one correspondence with infinite sequences $a_0, a_1, a_2, a_3, \ldots$ of elements of R. It is convenient to represent the element of $R[[x]]$ corresponding to an infinite sequence $a_0, a_1, a_2, \ldots$ by means of a *formal power series*

$$a_0 + a_1 x + a_2 x^2 + a_3 a^3 + \cdots .$$

A formal power series may be represented more compactly by the expression

$$\sum_{j=0}^{\infty} a_j x^j.$$

The operations of addition and multiplication defined on the ring $R[[x]]$ are those that one would naturally employ when adding and multiplying power series. And, because we have verified that the operations of addition and multiplication on $\hat{R}$ satisfy all the appropriate ring axioms, we can conclude immediately that $R[[x]]$ is a unital commutative ring.

It is a straightforward exercise to verify that the element $1_R - x$ of the ring $R[[x]]$ is invertible, and that the inverse of this element is represented by the formal power series $1_R + x + x^2 + x^3 + x^4 + \cdots$. (This corresponds to the result that

$$(1_R, -1_R, 0_R, 0_R, \ldots) \times (1_R, 1_R, 1_R, \ldots) = (1_R, 0_R, 0_R, \ldots)$$

in the ring $\hat{R}$.) More generally it is not difficult to verify that an element $\sum_{j=0}^{\infty} a_j x^j$ of the ring $R[[x]]$ is invertible in $R[[x]]$ if and only if $a_0 \neq 0_R$.

The polynomial ring $R[x]$ is a subring of $R[[x]]$. Indeed an element $\sum_{j=0}^{\infty} a_j x^j$ of the ring $R[[x]]$ of formal power series belongs to the polynomial ring $R[x]$ if and only if there exists some positive integer n such that $a_j = 0_R$ whenever $j > n$.

C-2 Remarks on the Definition and Basic Properties of Polynomial Rings

Many of the standard examples arising in Galois Theory concern polynomials with numerical coefficients. Now the set $\mathbb{C}[x]$ consisting of all polynomials in a single indeterminate x with complex coefficients is a unital commutative ring. This statement amounts to little more than the observation that there are well-defined operations of addition, subtraction and multiplication defined on the set $\mathbb{C}[x]$ of polynomials with complex coefficients, and that these algebraic operations on polynomials satisfy all the usual commutative, associative and distributive laws.

A unital subring of $\mathbb{C}$ is a set of complex numbers which contains the numbers 0 and 1, and contains the sum, difference and product of any two of its elements. If R is a unital subring of $\mathbb{C}$ then $R[x]$ is a unital subring of $\mathbb{C}[x]$, and therefore $R[x]$ is a unital commutative ring.

In particular, if K is a subfield of $\mathbb{C}$ then $K[x]$, the set of polynomials in a single indeterminate x with coefficients in K is closed under the operations of addition, subtraction and multiplication of polynomials, and moreover it contains the constant polynomials with values 0 and 1. This means that $K[x]$ is a unital subring of $\mathbb{C}[x]$, and thus $K[x]$ is a unital commutative ring.

Now, whilst Galois Theory arose out of the study of the solvability of polynomials with numerical coefficients, the theory can be applied more widely. It is appropriate to generalize the results so that they can be applied to study the solvability of polynomials with coefficients in any field K. This field K might be a subfield of the complex numbers. Alternatively it might be a field with a finite number of elements: it can be shown that, given any prime number p, and given any positive integer n, there exists a field with p^n elements. Moreover every finite field is of order p^n for some prime number p and positive integer n, and any two finite fields of the same order are isomorphic. There are also many interesting and useful examples of fields that are neither subfields of $\mathbb{C}$ nor finite fields. It is therefore appropriate to develop a theory that is applicable to polynomials with coefficients in any field K whatsoever.

Now whatsoever field K we choose as our field of coefficients, the set $K[x]$ of polynomials with coefficients in K is itself well-defined, and there are well-defined operations of addition, substraction and multiplication defined on $K[x]$. Moreover, $K[x]$, with these algebraic operations, has the structure of a unital commutative ring. A certain amount of effort is required in order to check out all the details of the proof of this fact, but the verifications are straightforward and obvious. One should note that polynomials $f(x)$ and $g(x)$ with coefficients in some field K are equal if and only if every coefficient of $f(x)$ is equal to the corresponding coefficient of $g(x)$.

Now each polynomial $f(x)$ with coefficients in K determines a function from the coefficient field K to itself which maps each element α of K to $f(\alpha)$. If $f(x) = c_0 + c_1x + \cdots + c_nx^n$, where $c_0, c_1, \ldots, c_n \in K$, then $f(\alpha) = c_0 + c_1\alpha + \cdots + c_n\alpha^n$. If K is a subfield of the field $\mathbb{C}$ of complex numbers then each polynomial with coefficients in K is determined by the corresponding function on K. However the corresponding result does not hold when the field K is finite. For example, let K is a finite field with p elements, where p is a prime number, and let $f(x) = 1_K x^p - 1_K x$. Then $f(\alpha) = 0$ for all $\alpha \in K$. Indeed the field K is isomorphic to the field of congruence classes of integers modulo p, and Fermat's Little Theorem ensures that every integer n satisfies the congruence $n^p \equiv n \pmod{p}$. But although the function $\alpha \mapsto f(\alpha)$ on K determined by the polynomial f is the zero function, the polynomial f itself is a non-zero polynomial. This example shows that it is necessary to distinguish between polynomials with coefficients in a field K and the functions from K to itself that are determined by evaluating that polynomial at elements of the coefficient field K. Therefore one cannot develop a theory of polynomials with coefficients in an arbitrary field K in which polynomials are regarded as functions from K to itself.

A more formal approach to the construction of the polynomial ring $K[x]$ is presented at some length in Subsection C-1. One can represent a polynomial with coefficients in some field K as an infinite sequence $(c_0, c_1, c_2, \ldots)$ of elements of K, where only finitely many terms in this sequence are non-zero. One can define appropriate operations of addition and multiplication on such sequences that represent the usual operations of addition and multiplication of polynomials. One can then carefully check that these operations satisfy all the axioms needed to ensure that $K[x]$ is a unital commutative ring. This exercise estabilishes the theory of polynomial rings on a sound and secure footing.

C-3 The Structure of Rings of Polynomials with coefficients in a Field

Let K be a field, and let $K[x]$ be the ring of polynomials in a single indeterminate x with coefficients in K.

Now given any two polynomials h and f with coefficients in the field K, where $f \neq 0$, there exist polynomials q and r such that $h = qf + r$ and either $r = 0$ or else $\deg r < \deg f$ (Lemma 3.1). One may regard q as the quotient polynomial and r as the remainder obtained when we divide the polynomial h by the polynomial g by an algorithm analogous to the 'long division' algorithm for dividing natural numbers.

Suppose, for example that

$$h(x) = x^4 - 2x^3 + 5x^2 + 4x + 7 \quad \text{and} \quad f(x) = x^2 + x - 7.$$

Then

$$\begin{aligned} x^4 - 2x^3 + 5x^2 + 4x + 7 &= x^2(x^2 + x - 7) - 3x^3 + 12x^2 + 4x + 7 \\ -3x^3 + 12x^2 + 4x + 7 &= -3x(x^2 + x - 7) + 15x^2 - 17x + 7 \\ 15x^2 - 17x + 7 &= 15(x^2 + x - 7) - 32x + 112 \end{aligned}$$

It follows that

$$x^4 - 2x^3 + 5x^2 + 4x + 7 = (x^2 - 3x + 15)(x^2 + x - 7) - 32x + 112.$$

Thus $h(x) = q(x)f(x) + r(x)$, where $q(x) = x^2 - 3x + 15$ and $r(x) = -32x + 112$. Moreover $\deg r < \deg q$.

Given any ideal I of the polynomial ring $K[x]$, there exists some polynomial f with coefficients in K which generates the ideal I (Lemma 3.2). Then

$$I = \{gf : g \in K[x]\}.$$

Many key results concerning polynomials with coefficients in a field may be deduced as corollaries of this absolutely fundamental result. First we summarize the proof of this basic result. The case when I is the zero ideal is trivial: we take $f = 0$ in that case. Suppose that I is a non-zero ideal of $K[x]$. We choose $f \in I$ so as to minimize the degree amongst non-zero polynomials in I. Let $h \in I$. Then $h = qf + r$ for some $q, r \in K[x]$, where either $r = 0$ or else $\deg r < \deg f$. The definition of ideals ensures that $r \in I$. It follows that the case where $r \neq 0$ and $\deg r < \deg f$ is ruled out, because f was chosen so as to minimize the degree amongst the non-zero elements of I. Therefore $r = 0$ and $h = qf$, as required.

The result just discussed in turn leads to an important result concerning coprime polynomials. Let $f_1, f_2, \ldots, f_k$ be polynomicals with coefficients in the field K. We say that these polynomials are *coprime* if there is no non-constant polynomial that divides every one of these polynomials.

Let $f(x)$ and $m(x)$ be polynomials with coefficients in the field K, and let I be the ideal of the polynomial ring $K[x]$ generated by f and m. Then

$$I = \{u(x)f(x) + v(x)m(x) : u, v \in K[x]\}.$$

(This observation follows directly on applying Lemma 2.5.) Now it follows from Lemma 3.2 (discussed above) that there exists some polynomial $d(x)$ with coefficients in K which generates the ideal I. This polynomial $d(x)$

then divides both $f(x)$ and $m(x)$. Moreover $d \in I$, and therefore there exist $g, k \in K[x]$ such that $d(x) = g(x)f(x) - k(x)m(x)$. Now suppose that f and m are coprime. Then this polynomial $d(x)$ must be a constant polynomial. We may in fact choose d to be the constant polynomial whose value is the identity element 1_K of the field K. Then $g(x)f(x) - k(x)m(x) = 1_K$. (This result is a special case of Theorem 3.3.)

A polynomial $m(x)$ with coefficients in the field K is said to be *irreducible* over K if the only divisors of $m(x)$ in the polynomial ring $K[x]$ are the constant polynomials and the constant multiples of the polynomial $m(x)$. It follows from this definition that a polynomial $m(x)$ with coefficients in K is irreducible over K if and only if $m(x)$ cannot be factored as a product of polynomials of lower degree with coefficients in K.

Let $m(x)$ and $f(x)$ be polynomials with coefficients in K. Suppose that m is irreducible over K and that m does not divide f. Then the polynomials m and f are coprime, and therefore there exist polynomials $g(x)$ and $k(x)$ with coefficients in K such that $g(x)f(x) - k(x)m(x) = 1_K$.

We can re-express this result in the language of congruence classes. Let f, h and m be polynomials with coefficients in some field K. If $f(x) - h(x)$ is divisible by $m(x)$ then we say that f and h are *congruent* modulo m, and we write $f(x) \equiv h(x)$ (mod. $m(x)$), or, more concisely, $f \equiv h$ (mod. m). Thus $f(x) \equiv h(x)$ (mod. $m(x)$) if and only if there exists some polynomial k with coefficients in K such that $f(x) - h(x) = k(x)m(x)$.

We may now restate the previous result as follows. Let $m(x)$ and $f(x)$ be polynomials with coefficients in K. Suppose that $m(x)$ is irreducible over K and that $f(x) \not\equiv 0_K$ (mod. $m(x)$). Then there exists some polynomial $g(x)$ with coefficients in K such that $f(x)g(x) \equiv 1_K$ (mod. $m(x)$).

Now let $m(x)$ be a polynomial with coefficients in K. Each polynomial $f(x)$ with coefficients in K then determines a congruence class modulo $m(x)$. This congruence class consists of all polynomials $h(x)$ with coefficients in K for which $h(x) \equiv f(x)$ (mod. $m(x)$). There are well-defined operations of addition, subtraction and multiplication defined on congruence classes: the sum, difference and product of the congruence classes of polynomials $f(x)$ and $g(x)$ are the congruence classes of $f(x) + g(x)$, $f(x) - g(x)$ and $f(x)g(x)$ respectively. The set of congruence classes of polynomials modulo $m(x)$, with these operations of addition, subtraction and multiplication of congruence classes, is then a unital commutative ring. This ring is in fact the quotient ring $K[x]/(m)$ where (m) denotes the ideal of $K[x]$ generated by the polynomial m.

Suppose now that the polynomial $m(x)$ is irreducible. Let $f(x)$ be a polynomial satisfying $f(x) \not\equiv 0_K$ (mod. $m(x)$). We have shown that there exists a polynomial $g(x)$ with coefficients in K such that $f(x)g(x) \equiv 1_K$. It

follows that the congruence class of $f(x)$ is invertible in the ring of congruence classes of polynomials modulo $m(x)$, and moreover the inverse of the congruence class of $f(x)$ is the congruence class of $g(x)$. It follows that if the polynomial $m(x)$ is irreducible over K then the ring of congruence classes of polynomials modulo $m(x)$ is a field. In other words, if the polynomial $m(x)$ is irreducible over K then the quotient ring $K[x]/(m)$ is a field. (This result is Proposition 3.6.)

C-4 Products of Primitive Polynomials and Eisenstein's Irreducibility Criterion

It should be clear that there are some basic ideas common to the proofs of Gauss's Lemma and Eisenstein's Irreducibility Criterion. We explore this ideas below.

Let $g(x)$ and $h(x)$ be polynomials with integer coefficients. We write

$$g(x) = \sum_{j=0}^{r} b_j x^j, \quad h(x) = \sum_{k=0}^{s} c_k x^k,$$

where $b_0, b_1, \ldots, b_r$ and $c_0, c_1, \ldots, c_s$ are integers. It is convenient to define $b_j = 0$ when $j > r$, and $c_k = 0$ when $k > s$. Then the coefficients b_j and c_k are defined appropriately for all non-negative integers j and k. Let p be a prime number. Suppose that the polynomials $g(x)$ and $h(x)$ each have at least one coefficient that is not divisible by p. Then these polynomials each have a coefficient that is of smallest order subject to being non-divisible by p. Thus there exist integers j_0 and k_0, where $0 \leq j_0 \leq r$ and $0 \leq k_0 \leq s$, such that b_{j_0} and c_{k_0} are not divisible by p, b_j is divisible by p for all integers j satisfying $0 \leq j < j_0$, and c_k is divisible by p for all integers k satisfying $0 \leq k < k_0$. We claim that the coefficient of $x^{j_0+k_0}$ in the product polynomial $g(x)h(x)$ is not divisible by p. Now

$$g(x)h(x) = \sum_{n=0}^{r+s} a_n x^n,$$

where

$$a_n = \sum_{j=0}^{n} b_j c_{n-j}$$

for $n = 0, 1, 2, \ldots, r+s$. Suppose that $n = j_0 + k_0$. Then a_n is the sum of the quantities $b_j c_k$ with $j + k = j_0 + k_0$. Note that if $j \neq j_0$ and $k = n - j$ then either $j < j_0$, in which case b_j is divisible by the prime number p, or

else $k < k_0$, in which case c_k is disivible by p. It follows that $a_{j_0+k_0} - b_{j_0}c_{k_0}$ is divisible by p. But $b_{j_0}c_{k_0}$ is not divisible by p, since p does not divide either b_{j_0} or c_{j_0}, and a prime number cannot divide a product of integers unless it divides at least one of the factors. We deduce from this that $a_{j_0+k_0}$ is not divisible by p.

We can summarize what we have so far established as follows.

> Let $g(x)$ and $h(x)$ be polynomials with integer coefficients, let p be a prime number, let j_0 be the smallest non-negative integer with the property that p does not divide the coefficient b_{j_0} of x^{j_0} in $g(x)$, and let k_0 be the smallest non-negative integer with the property that p does not divide the coefficient c_{k_0} of x^{k_0} in $h(x)$. Then p does not divide the coefficient of $x^{j_0+k_0}$ in the product polynomial $g(x)h(x)$.

It follows directly from this that if $g(x)$ and $h(x)$ are primitive polynomials then so is the product polynomial $g(x)h(x)$. Indeed if p is any prime number then p cannot divide all the coefficients of $g(x)$, and it cannot divide all the coefficients of $h(x)$ and therefore p cannot divide all the coefficients of $g(x)h(x)$. Gauss's Lemma follows from this observation.

Now we consider Eisenstein's criterion. Suppose that a polynomial $f(x)$ of degree m with integer coefficients factors as a product of the form $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials with integer coefficients. Let $f(x) = \sum_{n=0}^{m} a_n x^n$, where $a_m \neq 0$. Suppose that there exists some prime number p such that p does not divide the leading coefficient a_m of f, p divides the coefficient a_n for f for $0 \leq n < m$, and p^2 does not divide the constant coefficient a_0 of f. Let

$$g(x) = \sum_{j=0}^{r} b_j x^j, \quad h(x) = \sum_{k=0}^{s} c_k x^k.$$

Now the prime number p does not divide all of the coefficients of the polynomial $g(x)$, for if it did, it would then divide all of the coefficients of $f(x)$. Therefore there is some non-negative integer j_0 which is the smallest non-negative integer with the property that p does not divide b_{j_0}. Similarly there is some non-negative integer k_0 which is the smallest non-negative integer with the property that p does not divide c_{k_0}. It then follows from the discussion above that the prime number p does not divide $a_{j_0+k_0}$. But all coefficients of the polynomial f other than the leading coefficient are required to be divisible by this prime number p. Therefore $j_0 + k_0 = m$, where $m = \deg f$. Also b_0 and c_0 cannot both be divisible by p, since the constant coefficient a_0

of f is not divisible by p^2, and $a_0 = b_0 c_0$. Thus either $j_0 = 0$, or else $k_0 = 0$. These observations limit the possible values of j_0 and k_0: either $j_0 = m$ and $k_0 = 0$, or else $j_0 = 0$ and $k_0 = m$. Thus if the polynomial $f(x)$ satisfies the conditions in the statement of Eisenstein's Criterion, and if $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials with integer coefficients, then either $\deg g = \deg f$ or $\deg h = \deg f$. Thus a polynomial $f(x)$ with the properties specified in the statement of Eisenstein's criterion cannot be factored as a product of polynomials of lower degree with integer coefficients. It then follows from Gauss's Lemma that such a polynomial must be irreducible over the field $\mathbb{Q}$ of rational numbers.