Modern Algebra Lecture Notes: Rings and fields set 3

Kevin Broughan

University of Waikato, Hamilton, New Zealand

May 6, 2010

Definition

Let R be a commutative ring and x a "symbol" or "indeterminate". The by $R[x]$ we mean the set of formal sums

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0$$

where the $a_i \in R$. We abbreviate these expressions by $f(x), g(x) etc$ and call them polynomials in x with coefficients in R.

Operations in $R[x]$

We make $R[x]$ into a ring by defining addition and multiplication as though x was a real variable and the expressions $f(x)$, $g(x)$ were ordinary polynomial functions of x:

$$\begin{aligned}
f(x) &:= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0, \\
g(x) &:= b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x^1 + b_0, \\
f(x) + g(x) &:= \sum_{j=0}^{n} (a_j + b_j) x^j, \\
f(x).g(x) &:= \sum_{j=0}^{n} c_j x^j \text{ where } c_j = \sum_{i=0}^{j} a_i b_{j-i}.
\end{aligned}$$

Notes

(1) These expressions $f(x)$ are not functions, but become so if x is given values in a ring. Indeed , if $a \in R$ then the map $f \longrightarrow f(a)$ is a homomorphism $R[x] \longrightarrow R$.
(2) The a_i or b_i could be zero and that these operations emulate ordinary polynomial arithmetic.

(1) In $\mathbb{Z}[x]$, $f(x) = x + 1,\ g(x) = x^2 + 3 \implies f(x) + g(x) = (0 + 1)x^2 + (1 + 0)x + (1 + 3) = x^2 + x + 4$.

(2) In $\mathbb{Z}[x]$,
$f(x) = x+1,\ g(x) = x^2+3 \implies f(x).g(x) = (x+1)(x^2+3) = x^3+x^2+3x+3$.

(3) We write $c_j = \sum_{i=0}^{j} a_i b_{j-i} = a_0 b_j + a_1 b_{j-1} + \cdots + a_j b_0$, the Cauchy product. So in Example (2) the coefficient of x is $c_1 = a_0 b_1 + a_1 b_0 = 1.0 + 1.3 = 3$.

$R[x]$ is a commutative ring

There are all of the axioms to check. The zero polynomial $f(x) = a_0 = 0$ is the additive identity and if R has an identity 1, the identity of $R[x]$ is $f(x) = 1$, both constant polynomials.

$R[x]$ is commutative because firstly, in $f(x).g(x)$,

$$c_j = \sum_{i=0}^{j} a_i b_{j-i} = \sum_{i=0}^{j} b_{j-i} a_i$$

using the commutativity of R. Then re-index with $k = j - i$ so $i = j - k$ making

$$c_j = \sum_{k=0}^{j} b_k a_{j-k} = \sum_{i=0}^{j} b_i a_{j-i}$$

and this is just the j'th coefficient for $g(x).f(x)$.

That $f(x) + g(x) = g(x) + f(x)$, $f(x) + 0 = f(x)$, $1.f(x) = f(x)$ are easy, but good practice for becoming familiar with the notation.

Leading coefficient and degree

Definitions

The terms a_n are called coefficients and the coefficient which is non-zero with the highest value of n is called the leading coefficient, with the value of n being the degree of the polynomial. The zero polynomial has, by decree, no degree, and a constant non-zero polynomial degree 0. If the leading coefficient is 1, the polynomial is called monic.

Examples

(1) $f(x) = 0x^5 + 3x^4 + x^3 + x^2 - 2x - 3$ in $\mathbb{Z}[x]$ has leading coefficient 3, degree 4 and is not monic.

(2)$g(x) = 1$ has degree zero, $g(x) - g(x)$ has no degree.

(3) If $R = \mathbb{Z}/4Z$, $f(x) = 8x^5 + 5x^4 + 1$ has degree 4 and is monic.

(4) If $R = \mathbb{Q}[y]$ and $f(x) \in R[x]$ is defined as
$f(x) = (y^2 + 1/2)x^3 - yx + (y^4 - 3/4)$, then $f(x)$ has degree 3 and leading coefficient $y^2 + 1/2$ so is not monic.

If R is an integral domain so is $R[x]$

Proof

We have already seen that $R[x]$ is a commutative ring with 1. So let $a_m,\ b_n$ be the leading (non-zero) coefficients for the non-zero polynomials $f(x),\ g(x)$:

$$\begin{aligned} f(x) &:= a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x^1 + a_0, \\ g(x) &:= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x^1 + b_0. \end{aligned}$$

Then the coefficient of the highest possible power of x in $f(x).g(x)$ is

$$c_{m+n} = \sum_{i=0}^{m+n} a_i.b_{m+n-i} = a_m.b_n,$$

which, since R is an integral domain, is non-zero. (If $i < m,\ m+n-i > n$ so $b_{m+n-i} = 0$. If $i > m,\ a_i = 0$.) Therefore $R[x]$ is an integral domain.

Corollary

$\deg f(x).g(x) = m + n = \deg f(x) + \deg g(x)$.

Theorem 14 The division identity

If $F[x]$ is the ring of polynomials with coefficients in a field F and $f(x),\ g(x) \in F[x]$ with $g(x) \neq 0$ then there are unique polynomials $q(x),\ r(x)$ in $F[x]$ with

$$f(x) = q(x).g(x) + r(x),\ r(x) = 0 \text{ or } \deg r(x) < \deg g(x).$$

Note

This identity is vital for any treatment of polynomials in Modern Algebra. It represents the familiar division of one polynomial by another giving a remainder of lower degree than the divisor, when the division is not "exact". The "exact" case is when $g(x)$ "divides" $f(x)$.

Example

Divide $x^3 - x^2 + 2x - 3$ by $x - 2$:

$$
\begin{array}{rr|rcrcrcr}
 & & x^2 & + & x & + & 4 & & \\
\cline{3-9}
x-2 & \big| & x^3 & - & x^2 & + & 2x & - & 3 \\
 & & x^3 & - & 2x^2 & & & & \\
\cline{3-9}
 & & & & x^2 & + & 2x & - & 3 \\
 & & & & x^2 & - & 2x & & \\
\cline{5-9}
 & & & & & & 4x & - & 3 \\
 & & & & & & 4x & - & 8 \\
\cline{7-9}
 & & & & & & & & 5
\end{array}
$$

Hence, $x^3 - x^2 + 2x - 3 = (x - 2)(x^2 + x + 4) + 5$.

Proof of Theorem 14

We will first consider the existence of $q(x)$ and $r(x)$. Let $S = \{f(x) - g(x)h(x) : h(x) \in F[x]\}$ and assume that

$$g(x) = a_0 + a_1x + \cdots + a_nx^n$$

is a polynomial of degree n. This set is nonempty since $f(x) \in S$.

If $f(x)$ is the zero polynomial, then

$$0 = f(x) = 0 \cdot g(x) + 0;$$

hence, both q and r may be chosen as the zero polynomial.

Now suppose that the zero polynomial is not in S. In this case the degree of every polynomial in S is nonnegative. Choose a polynomial $r(x)$ of smallest degree in S; hence, there must exist a $q(x) \in F[x]$ such that

$$r(x) = f(x) - g(x)q(x),$$

or

$$f(x) = g(x)q(x) + r(x).$$

We need to show that the degree of $r(x)$ is less than the degree of $g(x)$. Assume that $\deg g(x) \leq \deg r(x)$. Say $r(x) = b_0 + b_1 x + \cdots + b_m x^m$ and $m \geq n$. Then

$$\begin{aligned} f(x) - g(x)[q(x) + (b_m/a_n)x^{m-n}] &= f(x) - g(x)q(x) \\ &\quad - (b_m/a_n)x^{m-n}g(x) \\ &= r(x) - (b_m/a_n)x^{m-n}g(x) \\ &= r(x) - b_m x^m \\ &\quad + \text{terms of lower degree} \end{aligned}$$

is in S.

This is a polynomial of lower degree than $r(x)$, which contradicts the fact that $r(x)$ is a polynomial of smallest degree in S; hence, $\deg r(x) < \deg g(x)$.

To show that $q(x)$ and $r(x)$ are unique, suppose that there exist two other polynomials $q'(x)$ and $r'(x)$ such that $f(x) = g(x)q'(x) + r'(x)$ and $\deg r'(x) < \deg g(x)$ or $r'(x) = 0$.

Assume $q(x) \neq q'(x)$. Then

$$f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x),$$

and

$$g(x)[q(x) - q'(x)] = r'(x) - r(x).$$

If g is not the zero polynomial, then

$$\deg g(x) \leq \deg(g(x)[q(x) - q'(x)]) = \deg(r'(x) - r(x)).$$

However, the degrees of both $r(x)$ and $r'(x)$ are strictly less than the degree of $g(x)$; therefore, $q(x) = q'(x)$ and so $r(x) = r'(x)$ also.