3.9 Polynomial Rings

Let F be a field. By the *ring of polynomials* in the indeterminate, x, written as $F[x]$, we mean the set of all symbols $a_0 + a_1x + \ldots + a_nx^n$, where n can be any nonnegative integer and where the coefficients $a_1, a_2, \ldots, a_n$ are all in F. In order to make a ring out of $F[x]$ we must be able to recognize when two elements in it are equal, we must be able to add and multiply elements of $F[x]$ so that the axioms defining a ring hold true for $F[x]$. This will be our initial goal.

We could avoid the phrase "the set of all symbols" used above by introducing an appropriate apparatus of sequences but it seems more desirable to follow a path which is somewhat familiar to most readers.

DEFINITION: If $p(x) = a_0 + a_1x + \ldots + a_mx^m$ and $q(x) = b_0 + b_1x + \ldots + b_nx^n$ are in $F[x]$, then $p(x) = q(x)$ if and only if for every integer $i \geq 0$, $a_i = b_i$.

Thus two polynomials are declared to be equal if and only if their corresponding coefficients are equal.

DEFINITION: If $p(x) = a_0 + a_1x + \ldots + a_mx^m$ and $q(x) = b_0 + b_1x + \ldots + b_nx^n$ are both in $F[x]$, then

$$p(x) + q(x) = c_0 + c_1x + \ldots + c_tx^t$$

where for each i, $c_i = a_i + b_i$.

In other words, add two polynomials by adding their coefficients and collecting terms. To add $1 + x$ and $3 - 2x + x^2$ we consider $1 + x$ as $1 + x + 0x^2$ and add, according to the recipe given in the definition, to obtain as their sum $4 - x + x^2$.

The most complicated item, and the only one left for us to define for $F[x]$, is the multiplication.

DEFINITION: If $p(x) = a_0 + a_1x + \ldots + a_mx^m$ and $q(x) = b_0 + b_1x + \ldots + b_nx^n$, then

$$p(x)q(x) = c_0 + c_1x + \ldots + c_kx^k$$

where

$$c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + \ldots + a_0b_t.$$

This definition says nothing more than: multiply the two polynomials by multiplying out the symbols formally, use the relation $x^\alpha x^\beta = x^{\alpha+\beta}$ and collect terms.

EXAMPLE: Let

$$p(x) = 1 + x - x^2, \quad q(x) = 2 + x^2 + x^3.$$

Here

$$a_0 = 1,\ a_1 = 1,\ a_2 = -1,\ a_3 = a_4 = \ldots = 0,$$

and

$$b_0 = 2,\ b_1 = 0,\ b_2 = 1,\ b_3 = 1,\ b_4 = b_5 = \ldots = 0.$$

Thus

$$\begin{aligned}
c_0 &= a_0b_0 = 1 \cdot 2 = 2,\\
c_1 &= a_1b_0 + a_0b_1 = 1 \cdot 2 + 1 \cdot 0 = 2,\\
c_2 &= a_2b_0 + a_1b_1 + a_0b_2 = (-1) \cdot 2 + 1 \cdot 0 + 1 \cdot 1 = -1,\\
c_3 &= a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = 0 \cdot 2 + (-1) \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 2,\\
c_4 &= a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4\\
&= 0 \cdot 2 + 0 \cdot 0 + (-1) \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 0,\\
c_5 &= a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5\\
&= 0 \cdot 2 + 0 \cdot 0 + 0 \cdot 1 + (-1) \cdot 1 + 1 \cdot 0 + 0 \cdot 0 = -1,\\
c_6 &= a_6b_0 + a_5b_1 + a_4b_2 + a_3b_3 + a_2b_4 + a_1b_5 + a_0b_6\\
&= 0 \cdot 2 + 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 + (-1) \cdot 0 + 1 \cdot 0 + 1 \cdot 0 = 0,\\
c_7 &= c_8 = \ldots = 0.
\end{aligned}$$

Therefore according to our definition,

$$(1 + x - x^2)(2 + x^2 + x^3) = c_0 + c_1x + c_2x^2 + \ldots = 2 + 2x - x^2 + 2x^3 - x^5.$$

If you multiply these together high-school style you will see that you get the same answer. Our definition of product is the one the reader has always known.

Without further ado we assert that $F[x]$ is a ring with these operations, its multiplication is commutative, and it has a unit element. We leave the verification of the ring axioms to the reader.

DEFINITION: If $f(x) = a_0 + a_1x + ... + a_nx^n \neq 0$ and $a_n \neq 0$ then the *degree* of $f(x)$, written as $\deg f(x)$, is n.

That is, the degree of $f(x)$ is the largest integer i for which the ith coefficient of $f(x)$ is not 0. We do not define the degree of the zero polynomial. We say a polynomial is a *constant* if its degree is 0. The degree function defined on the nonzero elements of $F[x]$ will provide us with the function $d(x)$ needed in order that $F[x]$ be a Euclidean ring.

LEMMA 3.9.1: *If $f(x), g(x)$ are two nonzero elements of $F[x]$, then*

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

Proof: Suppose that $f(x) = a_0 + a_1x + \ldots + a_mx^m$ and $g(x) = b_0 + b_1x + \ldots + b_nx^n$ and that $a_m \neq 0$ and $b_n \neq 0$. Therefore $\deg f(x) = m$ and $\deg g(x) = n$. By definition,

$$f(x)g(x) = c_0 + c_1x + \ldots + c_kx^k$$

where

$$c_t = a_tb_0 + a_{t-1}b_1 + \ldots + a_1b_{t-1} + a_0b_t.$$

We claim that $c_{m+n} = a_mb_n \neq 0$ and $c_i = 0$ for $i > m + n$. That $c_{m+n} = a_mb_n$ can be seen at a glance by its definition. What about c_i for $i > m + n$? c_i is the sum of terms of the form a_jb_{i-j}; since $i = j + (i - j) > m + n$ then either $j > m$ or $(i - j) > n$. But then one of a_j or b_{i-j} is 0, so that $a_jb_{i-j} = 0$; since c_i is the sum of a bunch of zeros it itself is 0, and our claim has been established. Thus the highest nonzero coefficient of $f(x)g(x)$ is c_{m+n} whence

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

COROLLARY: *If $f(x), g(x)$ are nonzero elements in $F[x]$ then* $\deg f(x) \leq \deg(f(x)g(x))$.

Proof: Since $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$, and since $\deg g(x) \geq 0$, this result is immediate from the lemma. ■

COROLLARY: *$F[x]$ is an integral domain.*

Proof: We leave the proof of this corollary to the reader.

Since $F[x]$ is an integral domain, in light of Theorem 3.6.1 we can construct for it its field of quotients. This field merely consists of all quotients of polynomials and is called the field of *rational functions* in x over F. The function $\deg f(x)$ defined for all $f(x) \neq 0$ in $F[x]$ satisfies

1. $\deg f(x)$ is a nonnegative integer.

2. $\deg f(x) \leq \deg(f(x)g(x))$ for all $g(x) \neq 0$ in $F[x]$.

In order for $F[x]$ to be a Euclidean ring with the degree function acting as the d-function of a Euclidean ring we still need that given $f(x), g(x) \in F[x]$, there exist $t(x), r(x)$ in $F[x]$ such that

$$f(x) = t(x)g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. This is provided us by

LEMMA 3.9.2 (THE DIVISION ALGORITHM): *Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$, then there exist two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that*

$$f(x) = t(x)g(x) + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof: The proof is actually nothing more than the "long-division" process we all used in school to divide one polynomial by another.

If the degree of $f(x)$ is smaller than that of $g(x)$ there is nothing to prove, for merely put $t(x) = 0,\ r(x) = f(x)$, and we certainly have that $f(x) = 0 \cdot g(x) + f(x)$ where $\deg f(x) < \deg g(x)$ or $f(x) = 0$.

So we may assume that $f(x) = a_0 + a_1x + \ldots + a_mx^m$ and $g(x) = b_0 + b_1x + \ldots + b_nx^n$ where $a_m \neq 0,\ b_n \neq 0$ and $m \geq n$.

Let

$$f_1(x) = f(x) - \frac{a_m}{b_n}x^{m-n}g(x).$$

Thus $\deg f_1(x) \leq m - 1$, so by induction on the degree of $f(x)$ we may assume that $f_1(x) = t_1(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. But then

$$f(x) - \frac{a_m}{b_n}x^{m-n}g(x) = t_1(x)g(x) + r(x),$$

from which, by transposing, we arrive at

$$f(x) = \left(\frac{a_m}{b_n}x^{m-n} + t_1(x)\right)g(x) + r(x).$$

If we put

$$t(x) = \frac{a_m}{b_n}x^{m-n} + t_1(x)$$

we do indeed have that $f(x) = t(x)g(x) + r(x)$ where $t(x), r(x) \in F[x]$ and where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. This proves the lemma. ■

This last lemma fills the gap needed to exhibit $F[x]$ as a Euclidean ring and we now have the right to say

THEOREM 3.9.1: *$F[x]$ is a Euclidean ring.*

All the results of Section 3.7 now carry over and we list these, for our particular case, as the following lemmas. It could be very instructive for the reader to try to prove these directly, adapting the arguments used in Section 3.7 for our particular ring $F[x]$ and its Euclidean function, the degree.

LEMMA 3.9.3: *$F[x]$ is a principal ideal ring.*

LEMMA 3.9.4: *Given two polynomials $f(x)$, $g(x)$ in $F[x]$ they have a greatest common divisor $d(x)$ which can be realized as $d(x) = \lambda(x)f(x) + \mu(x)g(x)$.*

What corresponds to a prime element?

DEFINITION: A polynomial $p(x)$ in $F[x]$ is said to be *irreducible* over F if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, then one of $a(x)$ or $b(x)$ has degree 0 (i.e., is a constant).

Irreducibility depends on the field; for instance the polynomial $x^2 + 1$ is irreducible over the real field but not over the complex field, for there $x^2 + 1 = (x + i)(x - i)$ where $i^2 = -1$.

LEMMA 3.9.5: *Any polynomial in $F[x]$ can be written in a unique manner as a product of irreducible polynomials in $F[x]$.*

LEMMA 3.9.6: *The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal if and only $p(x)$ is irreducible over F.*

In Chapter 5 we shall return to take a much closer look at this field $F[x]/f(p(x))$, but for now we should like to compute an example.

Let F be the field of rational numbers and consider the polynomial

$$p(x) = x^3 - 2$$

in $F[x]$. As is easily verified, it is irreducible over F, whence $F[x]/(x^3 - 2)$ is a field. What do its elements look like? Let $A = (x^3 - 2)$, the ideal in $F[x]$ generated by $x^3 - 2$.

Any element in $F[x]/(x^3 - 2)$ is a coset of the form $f(x) + A$ of the ideal A with $f(x)$ in $F[x]$. Now, given any polynomial $f(x) \in F[x]$, by the division algorithm,

$$f(x) = t(x)(x^3 - 2) + r(x),$$

where $r(x) = 0$ or $\deg r(x) < \deg(x^3 - 2) = 3$. Thus $r(x) = a_0 + a_1x + a_2x^2$ where a_0, a_1, a_2 are in F; consequently

$$f(x) + A = a_0 + a_1x + a_2x^2 + t(x)(x^3 - 2) + A = a_0 + a_1x + a_2x^2 + A$$

since $t(x)(x^3-2)$ is in A. Hence by the addition and multiplication in $F[x]/(x^3-2)$,

$$f(x)+A=(a_0+A)+a_1(x+A)+a_2(x+A)^2.$$

If we put $t=x+A$, then every element in $F[x]/(x^3-2)$ is of the form $a_0+a_1t+a_2t^2$ with a_0,a_1,a_2 in F. What about t? Since

$$t^3-2=(x+A)^3-2=x^3-2+A=A=0$$

(since A is the zero element of $F[x]/(x^3-2)$) we see that $t^3=2$. Also, if

$$a_0+a_1t+a_2t^2=b_0+b_1t+b_2t^2,$$

then

$$(a_0-b_0)+(a_1-b_1)t+(a_2-b_2)t^2=0,$$

whence $(a_0-b_0)+(a_1-b_1)x+(a_2-b_2)x^2$ is in $A=(x^3-2)$. How can this be, since every element in A has degree at least 3? Only if

$$(a_0-b_0)+(a_1-b_1)x+(a_2-b_2)x^2=0,$$

that is, only if $a_0=b_0,\ a_1=b_1,\ a_2=b_2$. Thus every element in $F[x]/(x^3-2)$ has a *unique* representation as $a_0+a_1t+a_2t^2$ where $a_0,a_1,a_2\in F$. By Lemma 3.9.6, $F[x]/(x^3-2)$ is a field. It would be instructive to see this directly; all that it entails is proving that if $a_0+a_1t+a_2t^2\neq 0$ then it has an inverse of the form $\alpha+\beta t+\gamma t^2$ Hence we must solve for $\alpha,\ \beta,\ \gamma$ in the relation

$$(a_0+a_1t+a_2t^2)(\alpha+\beta t+\gamma t^2)=1,$$

where not all of a_0,a_1,a_2 are 0. Multiplying the relation out and using $t^3=2$ we obtain

$$(a_0\alpha+2a_2\beta+2a_1\gamma)+(a_1\alpha+a_0\beta+2a_2\gamma)t+(a_2\alpha+a_1\beta+a_0\gamma)t^2=1$$

thus

$$a_0\alpha+2a_2\beta+2a_1\gamma=1,$$

$$a_1\alpha+a_0\beta+2a_2\gamma=0,$$

$$a_2\alpha+a_1\beta+a_0\gamma=0.$$

We can try to solve these three equations in the three unknowns α,β,γ. When we do so we find that a solution exists if and only if

$$a_0^3+2a_1^3+4a_2^3-6a_0a_1a_2\neq 0.$$

Therefore the problem of proving directly that $F[x]/(x^3-2)$ is a field boils down to proving that the only solution in *rational* numbers of

$$a_0^3+2a_1^3+4a_2^3=6a_0a_1a_2 \tag{1}$$

is the solution $a_0=a_1=a_2=0$. We now proceed to show this. If a solution exists in rationals, by clearing of denominators we can show that a solution exists where a_0,a_1,a_2 are integers. Thus we may assume that a_0,a_1,a_2 are integers satisfying (1). We now assert that we may

assume that a_0, a_1, a_2 have no common divisor other than 1, for if $a_0 = b_0 d$, $a_1 = b_1 d$, and $a_2 = b_2 d$, where d is their greatest common divisor, then substituting in (1) we obtain

$$d^3(b_0^3 + 2b_1^3 + 4b_2^3) = d^3(6b_0 b_1 b_2),$$

and so

$$b_0^3 + 2b_1^3 + 4b_2^3 = 6b_0 b_1 b_2.$$

The problem has thus been reduced to proving that (1) has no solutions in integers which are relatively prime. But then (1) implies that a_0^3 is even, so that a_0 is even; substituting $a_0 = 2\alpha_0$ in (1) gives us

$$4\alpha_0^3 + a_1^3 + 2a_2^3 = 6\alpha_0 a_1 a_2.$$

Thus a_1^3, and so, a_1 is even; $a_1 = 2\alpha_1$. Substituting in (1) we obtain

$$2\alpha_0^3 + 4\alpha_1^3 + a_2^3 = 6\alpha_0 \alpha_1 a_2.$$

Thus a_2^3, and so a_2, is even! But then a_0, a_1, a_2 have 2 as a common factor! This contradicts that they are relatively prime, and we have proved that the equation $a_0^3 + 2a_1^3 + 4a_2^3 = 6a_0 a_1 a_2$ has no rational solution other than $a_0 = a_1 = a_2 = 0$. Therefore we can solve for α, β, γ and $F[x]/(x^3 - 2)$ is seen, directly, to be a field.