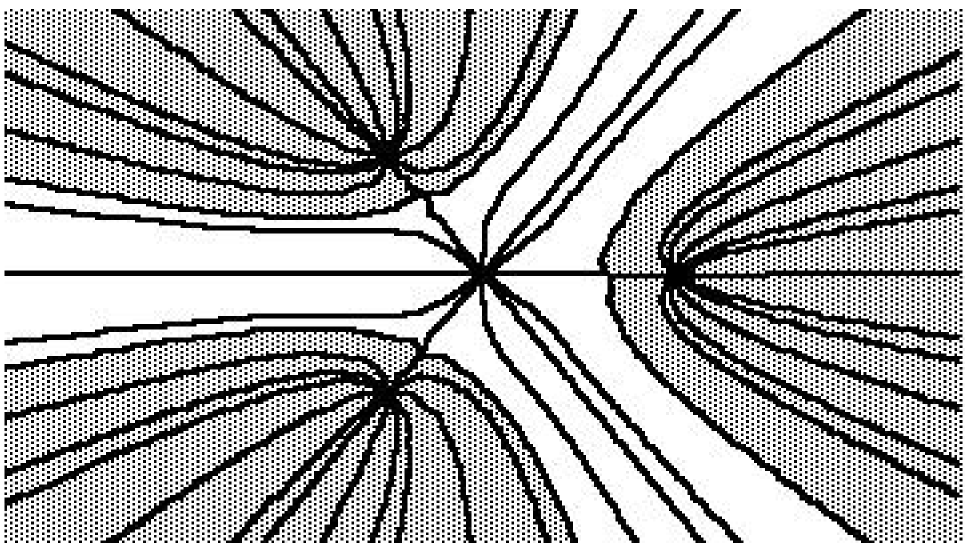
Theory of Equations

Lesson 2

by

Barry H. Dayton
Northeastern Illinois University
Chicago, IL 60625, USA

`www.neiu.edu/~bhdayton/theq/`



1.4 Polynomial Arithmetic

In this chapter a polynomial will be a function

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

where the numbers a_0, a_1, etc. are called the coefficients. We will attempt a more formal and precise definition in Chapter 5. The symbol x is simply a place holder, known as the ”variable.” The coefficients may be real or complex numbers, the set of all polynomial functions with real coefficients will be denoted $\boldsymbol{R}[x]$, the set of all polynomial functions with complex coefficients will be denoted $\boldsymbol{C}[x]$. A polynomial $p(x) \in \boldsymbol{R}[x]$ can be thought of either as a real-valued function of a real variable or a complex-valued function of a complex variable. Of course if $p(x) \in \boldsymbol{C}[x]$ has some imaginary coefficients we will generally only be able to think of $p(x)$ as a complex-valued function of a complex variable.

Specification of the coefficients is enough to specify a polynomial but the converse statement, i.e. that the function determines the coefficients, should not be taken as obvious. It is a theorem that will be proven later in this chapter.

We “evaluate” a polynomial by substituting an actual number (real or complex) for the variable x. There are good ways and not so good ways to do this. We will discuss the good ways in Chapter 2. Of course if you are using Maple the computer can worry about the details.

We add and multiply polynomial functions like functions in calculus, i.e. pointwise. Thus if $p(x), q(x)$ are polynomials, the *sum* is the polynomial $f(x)$ given by $f(x) = p(x) + q(x)$ for each x, and the *product* is $g(x)$ given by $g(x) = p(x) * q(x)$ for each x. Thus if $p(x), q(x)$ are polynomials with $p(3) = 7$ and $q(3) = -5$ then $(p + q)(3) = 2$ and $(p * q)(3) = -35$. We can also subtract polynomials, but we cannot divide as the quotient of two polynomial functions is no longer a polynomial function.

This arithmetic would not be particularly useful if it were not for the fact that one can fairly easily determine the coefficients of the sum and product from the summands and factors. It is an exercise with the associative, commutative and distributive laws of R and C to show that if

$$\begin{aligned} p(x) &= a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \\ q(x) &= b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \end{aligned}$$

then $p(x) + q(x) = f(x)$ and $p(x) * q(x) = g(x)$ where

$$\begin{aligned} f(x) &= c_0 + c_1x + \cdots + c_kx^k \\ g(x) &= d_0 + d_1x + \cdots + d_{m+m}x^{m+n} \end{aligned}$$

where $k = \max(m, n)$ and

$$\begin{aligned} c_i &= a_i + b_i \\ d_i &= \sum_{j=0}^{i} a_j b_{i-j}. \end{aligned}$$

Note that in the formula for multiplication we are assuming $a_i = 0$ for $i > n$, $b_j = 0$ for $j > m$. Multiplication is admittedly more complicated than addition, but this formula is forced upon us by (mostly) the distributive law.

It can be shown that addition and multiplication of polynomials satisfy the associative, commutative and distributive laws R1 - R5. The constant polynomial 0, i.e. the polynomial with all its coefficients 0, acts as a zero element while the constant polynomial 1, i.e. $p(x) = 1 + 0x + 0x^2 + \cdots$ is the multiplicative identity. Finally given a polynomial $p(x)$ there is a polynomial $q(x)$ such that $q(x) = -p(x)$ for each x; in particular, if

$$p(x) = a_0 + a_1 x + a_2 x_2 + \cdots + a_n x_n$$

then

$$q(x) = -a_0 - a_1 x - a_2 x^2 - \cdots - a_n x^n.$$

Thus $q(x)$ is an additive inverse to $p(x)$. It follows that $\boldsymbol{R}[x], \boldsymbol{C}[x]$ satisfy all the ring axioms. For this reason, instead of calling $\boldsymbol{R}[x], \boldsymbol{C}[x]$ *sets* of polynomials, we will call them *rings* of polynomials.

Maple Implementation

To define a polynomial one first chooses a *variable* or *indeterminant*, that is some letter that has not been assigned a numerical or other value. The letters `x,` `y` and `t` are good letters for this purpose, so you should avoid using these letters on the left side of an assignment statement `x :=` If, say x has been used as a value (local variables inside a procedure don't count) it can be "unassigned" by the command `x:= 'x'`

Polynomials are defined in a, more or less, obvious way. Don't forget that `:=` is used instead of the ordinary $=$. And don't forget to end each line with a semicolon. Thus to enter a polynomials $f(x) = x^3 - 2x^2 + 5$ and $g(x) = x^2 - x + 3$ type

```
f:= x^3 - 2*x^2 + 5;
g:= x^2 -x + 3;
```

Note that you must type `2*x^2` not `2x^2` even though Maple returns $2x^2$. This isn't actually fair but Maple is not as smart as you are and so needs help interpreting the expression `2x^2`.

To evaluate a polynomial, say f, at a number, say c, use the procedure

```
subs(x=c, f);
```

Do not set `x:= c` because this will destroy `x` as a variable and then f will simply be the number $f(c)$ and you will not be able to recover the *polynomial* f. c need not be an actual number, for instance c might be $\sqrt{2}$ and the result of `subs(x=sqrt(2),f);`, for $f = x^3 - 2x^2 + 5$ above would be $2\sqrt{2} + 1$, to get a decimal value use `evalf(subs(x=sqrt(2),f));` c may even be a variable expression, for example `subs(x=h+2, f);` returns h^3+4h^2+4h+5.

Now you can define the sum $h(x)$ and product $p(x)$ by

```
h := f + g;
p := f*g;
```

Don't be surprised if the results are

$$h := (x^3 - 2x^2 + 5) + (x^2 - x + 3)$$
$$p := (x^3 - 2x^2 + 5)(x^2 - x + 3)$$

There are procedures `normal, simplify, expand, sort` and `collect` which may change the algebraic form of your functions without changing the functions. Try them

```
h := normal(h);
h := simplify(h);
p := expand(p);
p := sort(p);
p := collect(p,x);
```

For getting polynomials into standard form $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ the most reliable of the above is `sort(collect(p,x))`. The `x` is the name of the variable that you want collected.

1.5 Degree

The *degree* of a polynomial $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is the largest index i for which the coefficient $a_i \neq 0$. Thus the polynomial $p(x) = 1 + x^2$ has degree 2. Constant polynomials have degree 0 with one exception: the constant polynomial 0, which has no non-zero coefficients does not have a degree. Alternatively, we can think of the 0 polynomial as having degree $-\infty$; this will make later results true so long as we accept the convention that $m + (-\infty) = -\infty$ for any integer m or $m = -\infty$.

We will denote the degree of a polynomial $p(x)$ by $\deg p(x)$.

Theorem 1.5.1 *Let* $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ *and* $q(x) = b_0 + b_1x + \cdots + b_mx^m$. *Assume* $\deg p(x) = n$ *and* $\deg q(x) = m$. *Then*

i) $\deg(p(x) + q(x)) \leq \max(n, m)$

ii) $\deg(p(x) * q(x)) = m + n$ *if* $p(x) \neq 0, q(x) \neq 0$

In particular we note that in the second formula that because of the definition of degree a_n, b_m are not 0; however a_i, b_j are 0 for $i > n, j > m$ so the coefficient d_{m+n} of $p(x) * q(x)$ is simply a_nb_m which is not zero by the axiom I1.

We thus note that for non-zero polynomials $p(x), q(x)$, the product $p(x) * q(x)$ has a degree and hence is also non-zero. Thus the polynomial rings $\boldsymbol{R}[x], \boldsymbol{C}[x]$ also satisfy axiom I1 and are thus *integral domains.*

On the other hand $\deg(p(x) * q(x)) \geq \deg p(x)$ so if $\deg p(x) \geq 1$ there is no way the product $p(x) * q(x) = 1$ since $\deg 1 = 0$. Hence the property in axiom F1 fails most of the time so division of polynomials in the sense of division of real numbers is not possible.

Maple Implementation

You can find the degree of the polynomial f by using the function `degree(f,x)`, the *leading* coefficient (the coefficient of the highest power of x with a non-zero coefficient) by `lcoeff(f,x)`, the *trailing* coefficient (the coefficient of the smallest power of x with non-zero coefficient, usually the constant term if this term is not zero) by `tcoeff(f,x)`. To find the coefficient of x^k use `coeff(f,x,k)`. In all of these `x` is the name of the variable.

1.6 The Division Algorithm

Although division in the sense of the real numbers is not possible, there is a very important type of division available, similar to the division of integers we learn in grade school. That is, the result of division of polynomials is not a polynomial but rather two polynomials, a quotient and a remainder. In fact, we will be generally more interested in the remainder. We state the fundamental fact as:

Theorem 1.6.1 (The Division Algorithm) *Given a polynomial* $p(x)$ *and a polynomial* $f(x)$ *with* $f(x) \neq 0$ *there exist unique polynomials* $q(x)$ *and* $r(x)$ *so that*

$$p(x) = f(x) * q(x) + r(x)$$

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

In this theorem, $p(x)$ is called the dividend, $f(x)$ the divisor, $q(x)$ the quotient, and $r(x)$ the remainder.

The Division Algorithm is strictly speaking a theorem rather than an algorithm. A theorem, such as 1.6.1, is a statement of mathematical fact whereas an algorithm is a procedure to perform a calculation. The actual division Algorithm is the procedure we learned in high school to actually find the quotient and the remainder; the Theorem 1.6.1 says that this procedure will always give an answer, and if two people independently perform the algorithm correctly they will both get the same answer. Historically this Theorem has been called the *Division Algorithm* and we must continue this tradition even though it conflicts with modern terminology.

In the special case when we divide $p(x)$ by $f(x)$ and get remainder $r(x) = 0$ we have the formula $p(x) = f(x) * q(x)$ and we say that $f(x)$ *divides* $p(x)$, or that $f(x)$ is a *factor* of $p(x)$. We write, in this case, $f(x)|p(x)$. Note carefully that the symbol | (*divides*) is a relation, not an operation, and thus the expression $f(x)|p(x)$ denotes either the word “true” or the word “false”, and not the quotient $q(x)$ which would be denoted by $p(x)/q(x)$, (we will avoid this latter notation for polynomials.)

Maple Implementation

MAPLE has functions to implement polynomial division. Given polynomials `p` the dividend and `f` the divisor, we find the quotient q by the statement `q:=quo(p,f,x);` and the remainder `r` by `r:=rem(p,f,x);` . The variable `x` must be listed as MAPLE allows `p,f` to have variables or expressions as coefficients.

The relation of divides is implemented by `divide(p,g)`. MAPLE interprets this correctly by returning the word "TRUE" if the remainder is 0 and "FALSE" otherwise.

Although we will have occasion to use arbitrary polynomials $f(x)$ as divisors, in most of our applications of the division theorem we will use the special case of $f(x) = x - c$ where c is a real or complex number. The reason is because of the following important theorem:

Theorem 1.6.2 (The Remainder Theorem) *Let $p(x)$ be a polynomial and $c \in \boldsymbol{C}$. Dividing $p(x)$ by the degree 1 polynomial $x - c$ gives as remainder the constant polynomial $p(c)$.*

Proof: We have $p(x) = (x - c)q(x) + r(x)$ by the Division Algorithm where $r(x) = 0$ or $\deg r(x) < \deg(x - c) = 1$; in either case $r(x)$ is a constant. Evaluating both sides at $x = c$ gives $p(c) = (c - c)q(c) + r(x) = r(x)$.

1.7 Factors and Roots.

Given a real or complex polynomial $p(x)$, a complex number c is called a *zero* or a *root* of $p(x)$ if $p(c) = 0$.

The following theorem is one of the most important results on polynomials. This result was first stated by the philosopher- mathematician Rene Descartes in Chapter 3 of his book *La Geometrie* published in 1637. The idea may have been known previously, but Descartes was the first to write polynomials as we do today and thus the first person capable of appropriately phrasing this result. *La Geometrie* is famous as the book in which analytic geometry first appears; however, Chapter 3 is actually the modern beginning of the Theory of Equations.

Theorem 1.7.1 (The Factor Theorem) *The complex number c is a root of $p(x)$ if and only if $(x - c)$ is a factor of $p(x)$.*

Proof: By the Remainder Theorem $p(x) = (x - c)q(x) + p(c)$ and thus $p(x) = (x - c)q(x)$ if and only if $p(c) = 0$.

For the polynomial $p(x) = x^2 - 2x + 1$ the number $c = 1$ is a root so $x - 1$ is a factor. But in this case, the other factor is also $x - 1$ so $p(x) = (x - 1)^2$. In this case we say $c = 1$ is a root of multiplicity 2.

More generally, we say c is a root of $p(x)$ of *multiplicity* k if $(x-c)^k$ divides $p(x)$ but $(x-c)^{k+1}$ does not. In other words, c is a root of $p(x)$ of multiplicity k if $p(x) = (x-c)^k q(x)$ and c is not a root of $q(x)$.

A consequence of the Factor Theorem is

Theorem 1.7.2 *If $p(x) \neq 0$ has degree n, then $p(x)$ has at most n roots, counted according to multiplicity.*

Proof: Use induction on n. The theorem is obvious for $n = 0, 1$. Suppose the theorem is true for all polynomials of degree less than n and $\deg p(x) = n$. Possibly $p(x)$ has no roots, which does not violate the conclusion of the theorem, but if $p(x)$ has a root of multiplicity k then $p(x) = (x-c)^k q(x)$ where $\deg q(x) = n - k \leq n$. By induction $q(x)$ has roots counted according to multiplicity of at most $n - k$ But by the integral domain property, roots of $p(x)$ are either c or roots of $q(x)$ so the total multiplicity is less than or equal to $k + (n-k) = n$.

We can now prove a result which implies one we took for granted earlier:

Theorem 1.7.3 *If $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ and $q(x) = b_0 + b_1 x + \cdots + b_m x^m$ are two polynomials with $p(x) = q(x)$ for all real (or complex) values of x then $\deg p(x) = \deg q(x)$ and $a_j = b_j$ for all j. In other words if $p(x) = q(x)$ as functions, their degrees and coefficients are equal.*

Proof: Suppose there is some j with $a_j \neq b_j$, then $f(x) = p(x) - q(x)$ has degree k where $k \geq j \geq 1$ (note $a_0 = p(0) = q(0) = b_0$ by hypothesis). By Theorem 1.7.2 $f(x)$ has at most k roots, but since $p(x) = q(x)$ for all x, $f(x)$ has infinitely many roots. This contradiction shows our original supposition to be wrong.

Theorem 1.7.2 says $p(x)$ of degree n has at most n roots, but if we are willing to consider complex roots the following theorem is actually true:

Theorem 1.7.4 (Fundamental Theorem of Algebra) *If $p(x) \in \boldsymbol{C}[x]$ has degree $n \geq 1$ then $p(x)$ has exactly n complex roots, counted according to multiplicity.*

We will devote Chapter 3 to a discussion of proofs of this theorem and related subjects. In the meantime we can use this when necessary.

Since the days of Al Khwarizmi mathematicians have devoted much thought and energy to the problem of actually finding the roots of polynomials. We will devote much of Chapters 2 and 4 to a discussion of the various methods used. The designers of the Maple already read these chapters so for the time being we can use Maple to find roots without worrying about how this is done.

Maple Implementation

Enter your polynomial as an expression as before, e.g.

```
f := 2 + 3*x - 5*xˆ2 + xˆ3 - xˆ4;
```

There are now three different solution methods at your disposal. To find *exact* solutions (see Chapter 4) type `solve(f=0,x);` . As you will see, this is probably not very useful for polynomials of degree 3 or higher, and Maple may not be able to find the roots for polynomials of degree 5 or larger. Sometimes Maple will give the solution in terms of the roots of a smaller degree polynomial in the form

```
         3
RootOf(_Z  + 3* _Z - 2)
```

Note that `_Z` is a dummy variable used by Maple and that this expression is actually the name of three separate numbers, i.e. the three complex roots of this polynomial.

If you are interested in floating point approximations for only the real roots type `fsolve(f=0,x);` . To get all the complex roots type `fsolve(f=0,x,complex);`. If you want to save and use these roots for something else use a syntax such as `y := fsolve(f=0,x,complex);` . Then `y` is an array variable containing all complex solutions, if you wish to use only the first use `y[1]` the second is `y[2]` and so on.