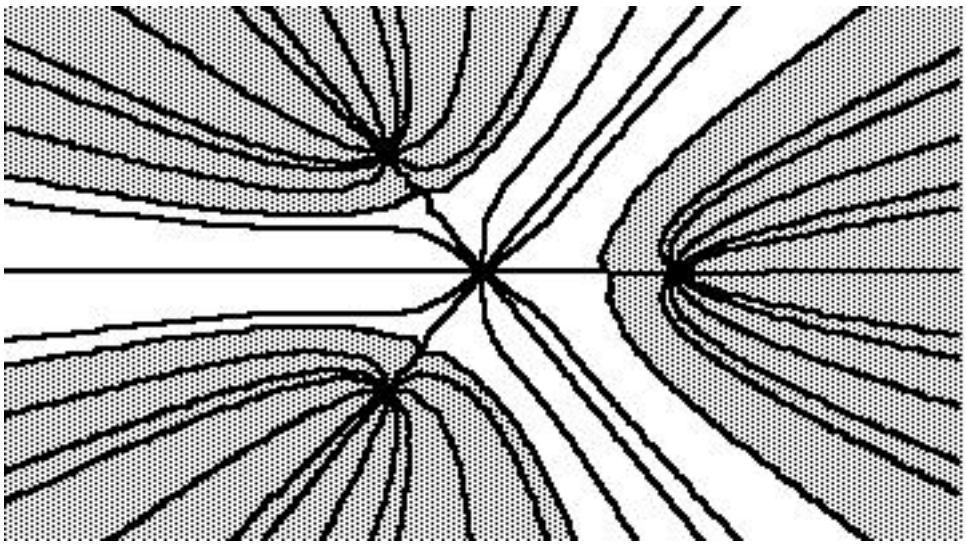
Theory of Equations

Lesson 3

by

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

www.neiu.edu/~bhdayton/theq/



1.8 Greatest Common Divisor

It would be easy, and not actually incorrect, to define the greatest common divisor of two polynomials $p(x), f(x)$ as a polynomial $g(x)$ of greatest degree which divides both $p(x)$ and $f(x)$. However simple, such a definition loses the essence of the notion of greatest common divisor; hence we go for a more complicated definition, but one which will bring important dividends later.

Definition 1.8.1 $g(x)$ is a greatest common divisor of $p(x), f(x)$ if

i) $g(x)$ divides both $p(x)$ and $f(x)$.

ii) If $h(x)$ is another polynomial which divides both $p(x)$ and $f(x)$, then $h(x)$ divides $g(x)$.

We write $g(x) = \gcd(p(x), f(x))$. The essential idea here is not that $g(x)$ is greatest in degree (which it is) but that $g(x)$ is greatest in terms of the relation "divides." One other point needs to be made at this time regarding the definition. Note that we said "g(x) is *a* greatest . . . " not "g(x) is *the* greatest . . . ." This is an important distinction; the gcd is not unique, there are many of them. For instance, given a gcd $g(x)$ and a constant $c \neq 0$, then $cg(x)$ is also a gcd. While this makes things a bit more complicated, it does give us some more flexibility. In particular, if $\gcd(f(x), g(x)) = c$ where $c \neq 0$ is a constant, we usually say $\gcd(f(x), g(x)) = 1$.

We now come to our theorem asserting existence of a gcd, and not only can we show that we can satisfy the condition in the definition, but in fact we have even more information about $g(x)$. This theorem is fairly technical and abstract, but it is very important, so we must prove it.

Theorem 1.8.2 *Given polynomials p(x), f(x) then a greatest common divisor $g(x)$ exists and is unique up to multiplication by a non-zero constant. Furthermore, there exist polynomials $u(x)$ and $v(x)$ so that*

$$g(x) = u(x) * p(x) + v(x) * f(x)$$

Proof: We consider the set of non-zero polynomials of the form $u(x) * p(x) + v(x) * f(x)$ as $u(x), v(x)$ range over all polynomials. We pick $g(x)$ to be a polynomial of this form of lowest degree. By the division theorem, $p(x) = g(x) * q(x) + r(x)$ where $\deg r(x) < \deg g(x)$. Then $r(x) = p(x) - g(x) * q(x) = p(x) - [u(x) * p(x) + v(x)f(x)] * q(x) = (1 - u(x) * q(x)) * p(x) + v(x) * q(x) * f(x)$. Since $g(x)$ had smallest

degree among all such non-zero polynomials, $r(x) = 0$ and thus $g(x)|p(x)$. Likewise $g(x)|f(x)$. If $h(x)|p(x)$ and $h(x)|f(x)$ then $p(x) = h(x) * a(x)$, $f(x) = h(x) * b(x)$ so $g(x) = u(x) * a(x) * h(x) + v(x) * b(x) * h(x) = (u(x) * a(x) + v(x) * b(x)) * h(x)$ so $h(x)|g(x)$. The uniqueness part is left as an exercise.

While this is a slick proof and establishes important properties of the gcd, it does not give one any help in actually finding a gcd – it is impractical to actually construct all polynomials of that form and look for a smallest one. Once again we have an algorithm, this one modelled on one used by Euclid to find the gcd of two line segments of integer length. First we prove a lemma.

Lemma 1.8.3 *Suppose* $p(x) = f(x)q(x) + r(x)$ *then*

$$\gcd(p(x), f(x)) = \gcd(f(x), r(x))$$

Proof: Let $g(x) = \gcd(f(x), p(x))$ and $h(x) = \gcd(f(x), r(x))$ where the $=$ sign is taken with a grain of salt since gcds are not unique. Then $g(x)|f(x)$ but since $r(x) = p(x) - f(x)q(x)$ it is easily seen that $g(x)|r(x)$. But by definition of $\gcd(f(x), r(x))$ we see that $g(x)|h(x)$. Likewise $h(x)|g(x)$. It follows from Theorem 1.5.1 that $\deg g(x) = \deg h(x)$ and thus, since $g(x)|h(x)$ that they are constant multiples of each other. But gcds are only defined up to constant multiple.

EUCLIDEAN ALGORITHM: Given polynomials $p(x), f(x)$ we apply the division algorithm repeatedly as follows:

$$\begin{aligned}
p(x) &= f(x) * q_1(x) + r_1(x) && \deg r_1(x) < \deg f(x) \\
f(x) &= r_1(x) * q_2(x) + r_2(x) && \deg r_2(x) < degr_1(x) \\
r_1(x) &= r_2(x) * q_3(x) + r_3(x) && \deg r_3(x) < degr_2(x) \\
&\vdots && \vdots \\
r_{k-2}(x) &= r_{k-1}(x) * q_k(x) + r_k(x) && \deg r_k(x) < \deg r_{k-1}(x) \\
r_{k-1}(x) &= r_k(x) * q_k(x) + r_{k+1}(x) && r_{k+1}(x) = 0
\end{aligned}$$

where eventually $r_j(x) = 0$ since the degrees of the $r_j(x)$ cannot continue to decrease indefinitely, the degrees being non-negative integers. By the Lemma, $\gcd(p(x), f(x)) = \gcd(f(x), r_1(x)) = \gcd(r_1(x), r_2(x)) = \cdots = \gcd(r_{k-1}(x), r_k(x)) = \gcd(r_k(x), 0) = r_k(x)$.

The extended version of the Euclidean Algorithm goes like this: For simplicity we drop the (x), i.e., write f instead of $f(x)$, etc. Define $r_{-1} = p, u_0 = 1, v_0 = 0$ and

$r_0 = f, u_1 = 0, v_1 = 1$ and for $n > 1$ define r_{n-1}, u_n, v_n recursively by setting q_n to be the quotient after dividing r_{n-3} by r_{n-2} and

$$\begin{aligned} r_{n-1} &= r_{n-3} - q_n r_{n-2} \\ u_n &= u_{n-2} - q_n u_{n-1} \\ v_n &= v_{n-2} - q_n v_{n-1} \end{aligned}$$

An easy induction argument shows that for each $n > 1$ that $\gcd(p, f) = \gcd(r_{n-1}, r_n)$ and

$$u_n p + v_n f = r_{n-1}$$

Thus if $r_k(x)$ is the last non-zero remainder

$$u_{k+1}(x)p(x) + v_{k+1}(x)f(x) = r_k(x) = \gcd(p(x), f(x))$$

Exercise 1.8.1 Once in each person's life one should calculate a greatest common divisor of two polynomials by hand, just so one appreciates the existence of computer programs to do this chore. Let $p(x) = x^4 + x^3 - 2x^2 + 17x - 5$ and $f(x) = x^4 - 3x^3 + 8x^2 - 7x + 5$. Find a greatest common divisor with integer coefficients; better yet, write this gcd in the form $u(x)p(x) + v(x)f(x)$.

The constant polynomial 1 (or any other non-zero constant polynomial, for that matter) divides any polynomial; thus if there is no common divisor of positive degree, 1 is a gcd. In this case we say that $p(x), f(x)$ are "relatively prime."

Maple Implementation

`g := gcd(p,f);` will give the gcd of polynomials `p,f` defined in the usual Maple fashion. If you need $u(x), v(x)$ you can use the extended gcd by `gcdex(p,f,x,'u','v');` where `p,f` are the polynomials, `x` is the variable and `'u', 'v'` are the names of the variables, enclosed in single quotes, which will evaluate to the desired $u(x), v(x)$.

1.9 Unique factorization

Definition 1.9.1 A polynomial $p(x)$ is called *irreducible* if it cannot be factored as the product of two polynomials of smaller degree.

Every polynomial of degree 0 or 1 is irreducible. A polynomial $p(x) \in \boldsymbol{R}[x]$ of degree 2 is irreducible if and only if it has no real roots, however no polynomial of degree 2 (or higher, if we accept the Fundamental Theorem) in $\boldsymbol{C}[x]$ is irreducible. Thus the irreducibility of a polynomial depends on the coefficient field we are using.

For technical reasons which will become more apparent in Chapter 5 we use the word *prime* to convey a slightly different meaning than "irreducible."

Definition 1.9.2 A polynomial $p(x)$ is called *prime* if $p(x)$ does not divide 1 and whenever $p(x)|f(x) * h(x)$ then either $p(x)|f(x)$ or $p(x)|h(x)$.

The technical condition "$p(x)$ does not divide 1" will be needed in Chapter 5; for now you should substitute the equivalent phrase "$\deg p(x) \geq 1$".

Theorem 1.9.3 *Let $p(x)$ be a polynomial in $\boldsymbol{R}[x]$ or $\boldsymbol{C}[x]$ of degree 1 or greater. Then $p(x)$ is prime if and only if $p(x)$ is irreducible.*

Proof: If $p(x)$ is prime it is easy to see that it is irreducible. Conversely, if $p(x)$ is irreducible and $p(x)|f(x)*h(x)$ suppose $p(x)$ does not divide $f(x)$. Let $gcd(p(x), f(x)) = g(x)$. Since $p(x)$ is irreducible, $g(x)$ has degree 0 or $\deg p(x)$. The second case is impossible (why – this is important!) thus we may take $g(x) = 1$. By Theorem 1.8.2 there are $u(x), v(x)$ with $1 = u(x) * p(x) + v(x) * f(x)$ so $h(x) = h(x) * u(x) * p(x) + v(x) * f(x) * h(x)$. But as $p(x)|f(x) * h(x), p(x)$ divides both terms of this last expression, hence $p(x)|h(x)$.

That last proof was surprisingly hard, but it is the key step in the proof of

Theorem 1.9.4 (Unique Factorization Theorem) *Any polynomial of degree greater or equal to 1 in $\boldsymbol{R}[x]$ or $\boldsymbol{C}[x]$ can be factored as a product of irreducible polynomials. The factors in different factorizations differ only as to order, constant multiples and constants.*

Example 1.9.5 If $p(x) = 3x^2 + 3x - 6$ then $p(x)$ may be factored as $(3x - 3) * (x + 2)$ or $(x - 1) * (3x + 6)$ or $3(x - 1) * (x + 2)$ or $-3 * (ix + 2i) * (ix - i)$ etc.

Sketch of proof: The existence of a factorization follows easily by induction on the degree and the definition of *irreducible*. The uniqueness assertion depends on the fact that the factors are *prime*. So if we have two different factorizations, each non-constant factor of the one divides some factor of the other. But since the factors are *irreducible* that factor of the first factorization must differ by the corresponding factor of the other by only a constant multiple.

Although the flexibility in factoring allowed by Theorem 1.9.4 may be useful in some situations, we often want to cut down the number of possible factorizations.

Definition 1.9.6 A polynomial $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ of degree n is called *monic* if $a_n = 1$.

It is clear (because of division of numbers) that any non-zero polynomial is a constant multiple of a monic polynomial. Thus Theorem 1.9.4 can be phrased as

Theorem 1.9.7 *Any polynomial of degree ≥ 1 in $\boldsymbol{R}[x]$ or $\boldsymbol{C}[x]$ can be factored as a product of monic irreducible polynomials multiplied by a constant. Any two such factorizations differ only by the order of the factors.*

We note that so far in this section we have not required the use of the Fundamental Theorem of Algebra, in fact we have used only the "field" properties of $\boldsymbol{R}$ and $\boldsymbol{C}$. Thus, Theorems 1.9.4 and 1.9.7 hold even if we restrict our coefficients (in both the polynomial to be factored and the factors) to rational numbers but, as we will see in Chapter 5, the irreducibles may be of any degree. However, assuming the Fundamental Theorem and allowing the coefficients of the factors to be in $\boldsymbol{C}$ or $\boldsymbol{R}$ gives particularly simple factorizations.

Theorem 1.9.8 *Let $p(x) \in \boldsymbol{C}[x]$ of degree $n \geq 1$. Then $p(x) = c(x - \alpha_1) * (x - \alpha_2) * \cdots * (x - \alpha_n)$ where $c \in \boldsymbol{C}$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the complex roots of $p(x)$ counted according to multiplicity.*

Before looking at factorizations over $\boldsymbol{R}$ we need to make a few comments. First, a degree 2 polynomial (called a quadratic) $ax^2 + bx + c$ is factorable in $\boldsymbol{R}[x]$ if and only if its roots are real, i.e. by the quadratic formula if and only if $b^2 - 4ac \geq 0$. If $p(x)$ is a real polynomial and α is an imaginary root, $p(\alpha) = 0$. But then $p(\bar{\alpha}) = \overline{p(\alpha)} = \bar{0} = 0$ by the properties of conjugation we discussed in §1.3 so $\bar{\alpha}$ is the other root. Combining the factors $(x - \alpha), (x - \bar{\alpha})$ of the factorization of Theorem 1.9.8 shows that $(x-\alpha)*(x-\bar{\alpha}) = x^2 - 2Re(\alpha)x + |\alpha|^2$ is a real factor of $p(x)$. All the imaginary roots pair up like this so we have

Theorem 1.9.9 (D'Alembert's Theorem) *Every real polynomial can be factored as a product of monic real linear (degree 1) polynomials times a product of real monic irreducible quadratics times a real constant. This factorization is unique except for the order of the factors.*

Example 1.9.10 Let $p(x) = x^3 - 2$. As a rational polynomial $p(x)$ is irreducible, as a real polynomial $p(x)$ factors as $(x - \sqrt[3]{2}) * (x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ while as a complex polynomial $p(x)$ factors as

$$p(x) = (x - \sqrt[3]{2}) * (x - \sqrt[3]{2}\frac{1 + \sqrt{3}i}{2}) * (x - \sqrt[3]{2}\frac{1 - \sqrt{3}i}{2})$$

One consequence of this, which also can be proven directly by use of the Intermediate Value Theorem of Calculus, is

Theorem 1.9.11 *Every real polynomial of odd degree has at least one real root.*

Maple Implementation

To do the kind of factoring discussed in this section use Maple's `factor(f, real);` or `factor(f, complex);` Important: if `f` is a Maple polynomial with integer or rational coefficients, the Maple function `factor(f);` without specifying rea or complex, will factor `f` into a product of polynomials with integer or rational coefficients. This is a completely different situation than we have been discussing here; a full discussion of this kind of factorization can be found in Chapter 5.

1.10 Formal Differentiation of Polynomials

Around 1680 Isaac Newton and Gottfried Leibniz invented the differential and integral calculus more or less independently. Both assumed that all functions could be expressed as power series which, since the notion of convergence hadn't yet been developed, were treated simply as big polynomials. We now know that this is not accurate, however many functions can be approximated by polynomials.

Interpreting Newton and Leibniz from a modern point of view, Newton defined for each polynomial a derivative polynomial as follows: given $p(x)$ we consider the function

$$F(x, h) = \frac{p(x + h) - p(x)}{h}$$

where h is a second variable. Applying the Binomial Theorem to each term of $p(x + h)$ in the numerator we see that $F(x, h)$ is actually a polynomial in x and h. Thus Newton defined $p'(x) = F(x, 0)$ (although he didn't use this notation, of course). Leibniz did

not give an algebraic description of the derivative but rather gave rules for finding the differential dp of a polynomial $p(x)$. The derivative is then $p'(x) = dp/dx$. Leibniz's rules (which are actually still called the Leibniz Rules today) include

$$\begin{aligned} dc &= 0 \qquad (c \text{ a constant}) \\ d(p+q) &= dp + dq \\ d(cp) &= cdp \qquad (c \text{ a constant}) \\ d(pq) &= pdq + qdp \\ dx^n &= nx^{n-1}dx \end{aligned}$$

It can be easily shown that Newton's construction satisfies Leibniz's rules and therefore both give the same derivative function. In fact, if $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ then $p'(x) = a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1}$. This rule works for both real and complex (or even rational) polynomials. In the complex (and rational) case we should interpret this algebraically as Newton and Leibniz did and forget calculus for the time being. The derivative $p'(x)$ of a polynomial $p(x)$ is also a polynomial and so has itself a derivative $p''(x)$ which in turn has a derivative $p'''(x) = p^{(3)}(x)$ and so on. Each differentiation lowers the degree by one so if $\deg p(x) = n$ then $p^{(n)}(x)$ is a constant and $p^{(k)}(x) = 0$ for $k > n$. In the next chapter we will give a powerful calculating technique called Horner's process for calculating derivatives at a point. It is based on the following simple theorem:

Theorem 1.10.1 *Let $p(x)$ be a (rational, real or complex) polynomial, c a complex number. By the Remainder theorem $p(x) = (x-c) * q(x) + p(c)$. Then $p'(c) = q(c)$.*

Maple Implementation

To find the formal derivative of a polynomial $f(x)$ use `diff(f, x)` . To evaluate at a point c use `subs(x=c, diff(f,x));`

1.11 Test for multiple roots

Theorem 1.11.1 *Let $p(x)$ be a polynomial, c a complex root of $p(x)$. Then c has multiplicity greater than 1 if and only if $p'(c) = 0$.*

Proof Since c is a root, by the Factor Theorem, $p(x) = (x - c) * q(x)$, as a complex polynomial. By Theorem 1.10.1, $p'(c) = q(c)$ so $p'(c) = 0$ if and only if c is a root of $q(x)$, i.e., if and only if $(x - c)$ is a factor of $q(x)$. But this is what is meant by multiplicity greater than 1.

An induction argument can be used to show that c is a root of multiplicity m if and only if $p(c) = p'(c) = \cdots = p^{(m-1)}(c) = 0$ but $p^{(m)}(c) \neq 0$.

A useful fact is that we can test to see if a polynomial has multiple roots without knowing what the roots are.

Theorem 1.11.2 (Multiple root test) *The non-constant polynomial $p(x)$ has no complex multiple roots if and only if $gcd(p(x), p'(x)) = 1$.*

Proof Let $\gcd(p(x), p'(x)) = g(x)$. If $g(x) \neq 1$ then $\deg g(x) \geq 1$ so $g(x)$ has a complex root c (here we are assuming the Fundamental Theorem). Since $g(x)|p(x)$ and $g(x)|p'(x)$ we see that c is a root of $p(x)$ and $p'(x)$ and thus by 1.11.1 c is a multiple root of $p(x)$.

For the converse, note that $g(x) = u(x) * p(x) + v(x) * p'(x)$ for some polynomials $u(x), v(x)$. Thus if c is a multiple root of $p(x)$, by 1.11.1 $p(c) = p'(c) = 0$ so $g(c) = 0$. But then $g(x)$ is not the constant 1.

In the complex case this theorem is innocent enough and in fact could be easily proven directly from Theorem 1.9.8. In fact, we see from the factorization of $p(x)$ that if $\alpha_1, \alpha_2, \ldots, \alpha_k$ are the multiple roots of $p(x)$ with α_j having multiplicity $m_j > 1$ then $gcd(p(x), p'(x))$ is the product of the $(x - \alpha_j)$ raised to the $m_j - 1$ power.

However when $p(x)$ is a real (or rational) polynomial, Theorem 1.11.2 hints at some of the deepest properties of roots. For if $p(x)$ is real (or rational) then so is $p'(x)$ and by the Euclidean Algorithm, so is $g(x) = gcd(p(x), p'(x))$. But by unique factorization, $g(x)$ is a product of irreducible factors of $p(x)$. We thus get the following amazing result:

Theorem 1.11.3 *Let $p(x)$ be a real (or rational) polynomial and $f(x)$ be an irreducible factor. If one root c of $f(x)$ has multiplicity m as a root of $p(x)$ then every root of $f(x)$ has multiplicity m as a root of $p(x)$. Further, if $p(x)$ is itself irreducible over $\boldsymbol{R}$ (or over the rationals) then $p(x)$ does not have multiple roots.*

1.12 Partial Fraction Decomposition

In this optional section we give a proof of the theorem guaranteeing partial fraction expansion for polynomials over the reals. The main application for this is to do closed form integration of rational functions. It was towards this end that D'Alembert pursued his version of the Fundamental Theorem of Algebra. In modern mathematics partial fraction decomposition is more likely to be used in combinatorial analysis where "generating functions" are obtained by finding "formal power series" representation of rational functions.

Both of the above applications require knowing the *exact* rather than numerical factorization of a polynomial; thus we must treat seriously the possibility of multiple roots and factors.

Theorem 1.12.1 (Partial Fractions Decomposition) *Let $\frac{f(x)}{g(x)}$ be a rational function where $f(x)$, $g(x)$ are polynomials over $\boldsymbol{R}$, and suppose $\deg f(x) < \deg g(x)$. Suppose over $\boldsymbol{R}$ $g(x)$ factors into irreducible factors (we can assume $g(x)$ is monic) as*

$$g(x) = (x-a_1)^{e_1}(x-a_2)^{e_2}\cdots(x-a_k)^{e_k}(x^2+b_1x+c_1)^{d_1}\cdots(x^2+b_mx+c_m)^{d_m}$$

Then $\frac{f(x)}{g(x)}$ is the sum of rational functions of the form

$$\frac{A_{ij}}{(x-a_i)^j}$$

where $i = 1, \ldots, k, j = 1, \ldots, e_i$, $A_{ij} \in \boldsymbol{R}$ and of the form

$$\frac{B_{ij}x + C_{ij}}{(x^2+b_ix+c_i)^j}$$

where $i = 1, \ldots, m$, and $j = 1, \ldots, d_j$.

The restriction that $\deg f(x) < \deg g(x)$ is not signficant because otherwise using the division algorithm we can divide $f(x)$ by $g(x)$ and get a polynomial plus a rational function of the right type. Thus a more general form of Partial Fractions Decomposition would say that any rational function is a polynomial plus a sum of rational functions of the type

$$\frac{A}{(x-a)^j} \text{ and } \frac{Bx+C}{(x^2+bx+c)^j}$$

Intuitively, the Partial Fractions Decomposition theorem is clear. If we write our rational function as a formal sum of rational functions of the type above and then multiply

both sides of the equation by $g(x)$, we have a polynomial equation where the left-hand side has degree less than or equal to $n-1$ where $\deg g(x) = n$ and the right-hand side has degree exactly $n-1$. Moreover, the coefficients on the left hand side are linear combinations of the A_{ij}, B_{ij} and C_{ij}. There are exactly n of these coefficients so equating the coefficients of $x^i, i = 0 \ldots n-1$ on both sides of the equation gives a system of n equations in n unknowns. In practice, we solve this system to find the coeffiecients of the Partial Fractions Decomposition. Unfortunately it is not obvious that this system is non-singular, so we will need a different proof.

Example 1.12.2 We consider the partial fraction decomposition of

$$Q(x) = \frac{x^5 - 6\,x + 9}{(\,x-3\,)^3\,(\,x^2+3\,x+5\,)^2}$$

We wish to write this in the form

$$\frac{A_1}{x-3} + \frac{A_2}{(\,x-3\,)^2} + \frac{A_3}{(\,x-3\,)^3} + \frac{B_1\,x + C_1}{x^2+3\,x+5} + \frac{B_2\,x + C_2}{(\,x^2+3\,x+5\,)^2}$$

We set $Q(x)$ equal to this and multiply both sides by the denominator of $Q(x)$ to get

$$\begin{aligned} x^5 - 6\,x + 9 = {} & (\,B_1 + A_1\,)\,x^6 + (\,A_2 + C_1 - 6\,B_1\,)\,x^5 \\ & + (\,A_3 - 8\,A_1 + 3\,A_2 - 6\,C_1 + B_2 + 5\,B_1\,)\,x^4 \\ & + (\,A_2 + 6\,A_3 - 30\,A_1 + C_2 + 9\,B_1 + 5\,C_1 - 9\,B_2\,)\,x^3 \\ & + (\,-9\,C_2 - 27\,A_2 + 9\,C_1 + 27\,B_2 + 19\,A_3 + 54\,B_1 + 16\,A_1\,)\,x^2 \\ & + (\,-135\,B_1 - 27\,B_2 - 65\,A_2 + 54\,C_1 + 27\,C_2 + 120\,A_1 + 30\,A_3\,)\,x \\ & + 25\,A_3 - 135\,C_1 + 225\,A_1 - 75\,A_2 - 27\,C_2 \end{aligned}$$

Now setting the coefficients of x^i equal on both sides of the equation we get the seven linear equations in seven unknowns

$$\begin{aligned} B_1 + A_1 &= 0 \\ A_2 + C_1 - 6\,B_1 &= 1 \\ A_3 - 8\,A_1 + 3\,A_2 - 6\,C_1 + B_2 + 5\,B_1 &= 0 \\ A_2 + 6\,A_3 - 30\,A_1 + C_2 + 9\,B_1 + 5\,C_1 - 9\,B_2 &= 0 \\ -9\,C_2 - 27\,A_2 + 9\,C_1 + 27\,B_2 + 19\,A_3 + 54\,B_1 + 16\,A_1 &= 0 \\ -135\,B_1 - 27\,B_2 - 65\,A_2 + 54\,C_1 + 27\,C_2 + 120\,A_1 + 30\,A_3 &= -6 \\ 25\,A_3 - 135\,C_1 + 225\,A_1 - 75\,A_2 - 27\,C_2 &= 9 \end{aligned}$$

These can be solved by your favorite linear equation solution method, but we recommend MAPLE's `solve` to get solutions represented as fractions. Thus

$$Q(x) = \frac{23742}{279841}\,\frac{1}{x-3} + \frac{4965}{12167}\,\frac{1}{(\,x-3\,)^2} + \frac{234}{529}\,\frac{1}{(\,x-3\,)^3} + \frac{-\frac{23742}{279841}\,x + \frac{23194}{279841}}{x^2+3\,x+5} + \frac{-\frac{807}{12167}\,x - \frac{9304}{12167}}{(\,x^2+3\,x+5\,)^2} \quad (1.1)$$

Of course, one could simply use MAPLE's `convert(Q,parfrac,x,true)` to get the same result directly.

To prove the partial fraction decomposition we first consider the case where $Q(x) = \frac{f(x)}{p(x)(q(x)}$ where $p(x), q(x)$ are relatively prime. Then by Theorem 1.8.2 there exist polynomials $u(x), v(x)$ with

$$u(x)p(x) + v(x)q(x) = 1$$

We then have

$$Q(x) = \frac{f(x)}{p(x)q(x)} = \frac{f(x)(u(x)p(x)+v(x)q(x)}{p(x)q(x)} = \frac{f(x)u(x)}{q(x)} + \frac{f(x)v(x)}{p(x)}$$

Continuing in this manner we write $Q(x)$ as a sum of rational functions where the denominators can not be factored into relatively prime factors, i.e. the denominators are powers of an irreducible polynomial.

Now assume we have a rational function of the form $\frac{f(x)}{p(x)^m}$ where $p(x)$ is irreducible. What we do is to divide $f(x)$ by $p(x)$ to get

$$f(x) = q_0(x)p(x) + r_0(x)$$

then divide $q_0(x)$ by $p(x)$ to get

$$q_0(x) = q_1(x)p(x) + r_1(x)$$

and so on until we get

$$\vdots$$
$$q_{m-2}(x) = q_{m-1}(x)p(x) + r_{m-1}(x)$$

Putting these together we have

$$f(x) = p(x)^m q_{m-1}(x) + p(x)^{m-1} r_{m-1}(x) + \cdots + p(x)r_1(x) + r_0(x)$$

so dividing by $p(x)^m$ we have the proper form

$$\frac{f(x)}{p(x)^m} = q_{m-1}(x) + \frac{r_{m-1}(x)}{p(x)} + \cdots + \frac{r_1(x)}{p(x)^{m-1}} + \frac{r_0(x)}{p(x)^m}$$

where the first term is a polynomial and all the numerators have degree less than that of $p(x)$.

Thus we have a two-step procedure for partial fraction decomposition. In step 1 we break up our rational function as a sum of rational fuctions where the denominators are powers of distinct irreducible polynomials. Step 2 writes each summand as a sum of a polynomial and fractions of the form $\frac{r(x)}{p(x)^j}$ where $\deg r(x) < \deg p(x)$ and $p(x)$ was our irreducible. Adding these expressions and combining the polynomial parts gives our final partial fraction decomposition. The reader should note that even though our original polynomial may have had numerator smaller than denominator, the summands in step 1 may not and the polynomial parts in step 2 may be non-zero. What must happen in this case is that the polynomial parts from each summand of step 1 must cancel off.

Example 1.12.3 Consider

$$Q(x) = \frac{x^5 - 6\,x + 9}{(\,x-3\,)^3\,(\,x^2+3\,x+5\,)^2}$$

of the earlier example. Writing $p = p(x) = x - 3$ and $q = q(x) = x^2 + 3x + 5$ so that $Q = \frac{f}{p^3q^2}$. Since $\gcd(p^3, q^2) = 1$ it follows that there exist polynomials a, b so that $a * p^3 + b * q^2 = 1$. In fact by the Euclidean Algorithm we have

$$a = -\frac{201\,x}{12167} - \frac{7083}{279841} - \frac{197\,x^3}{279841} - \frac{1359\,x^2}{279841}$$
$$b = \frac{3544}{279841} + \frac{197\,x^2}{279841} - \frac{1596\,x}{279841}$$

Thus

$$\begin{aligned} Q = \frac{f}{p^3q^2} = \frac{f(ap^3+bq^2)}{p^3q^2} &= \frac{fb}{p^3} + \frac{fa}{q^2} \\ &= \frac{\frac{197\,x^7}{279841} - \frac{1596\,x^6}{279841} + \frac{3544\,x^5}{279841} - \frac{1182\,x^3}{279841} + \frac{11349\,x^2}{279841} - \frac{35628\,x}{279841} + \frac{31896}{279841}}{(x-3)^3} \\ &\quad + \frac{\frac{197\,x^7}{279841} - \frac{1596\,x^6}{279841} + \frac{3544\,x^5}{279841} - \frac{1182\,x^3}{279841} + \frac{11349\,x^2}{279841} - \frac{35628\,x}{279841} + \frac{31896}{279841}}{(x^2+3x+5)^2} \end{aligned}$$

Next we write $fb = p^3 r_3 + p^2 r_2 + p r_1 + r_0$ where r_0, r_1, r_3 are of degree less than p, i.e. are constants. This is done by dividing fb by p, then dividing the quotient by p and the next quotient by p with r_0, r_1, r_2 the successive remainders and r_3 the last quotient. We get

$$
\begin{aligned}
r_0 &= \frac{234}{529} \\
r_1 &= \frac{4965}{12167} \\
r_2 &= \frac{23742}{279841} \\
r_3 &= \frac{197\,x^4}{279841} + \frac{177\,x^3}{279841} - \frac{182\,x^2}{279841} - \frac{1098\,x}{279841} - \frac{1371}{279841}
\end{aligned}
$$

Likewise we write $fa = q^2 s_2 + q s_1 + s_0$ where s_0, s_1 are the successive remainders on dividing first fa by q and then the quotient of the first division by q and s_2 is the quotient of the second division. We have

$$
\begin{aligned}
s_0 &= -\frac{807\,x}{12167} - \frac{9304}{12167} \\
s_1 &= -\frac{23742\,x}{279841} + \frac{23194}{279841} \\
s_2 &= -\frac{197\,x^4}{279841} - \frac{177\,x^3}{279841} + \frac{182\,x^2}{279841} + \frac{1098\,x}{279841} + \frac{1371}{279841}
\end{aligned}
$$

What we notice is that when we add $\frac{fb}{p^3}$ to $\frac{fa}{q^2}$ then r_3 and s_2 cancel out and we are left with precisely the formula of equation (1.1).

1.13 The Resultant

No book on Theory of Equations would be complete without at least mentioning the *resultant* of two polynomials. In this optional section we will do just that, mention the resultant. We will let the reader look up the details in a classical Theory of Equations text or in a good algebra book such as the one by S. Lang.

The problem is to decide if two polynomials $f(x), g(x)$ have a common root. In practice, if the coefficients of the polynomials are given numbers, the easiest way to solve this problem is to use a numerical algorithm to find the complex roots of the polynomials and see if any are the same. For example the procedure `fsolve` of MAPLE will work. If it appears that the two polynomials have the same root but you are not sure

then you could compute the greatest common divisor $h(x) = \gcd(f(x), g(x))$. If $h(x)$ is not a constant then the roots of $h(x)$ are the common roots. However, in some theoretical situations (for instance the coefficients may not be explicit numbers) a different criterion may be helpful. One then uses the resultant.

Let $f = f(x) = v_0x^n + v_1x^{n-1} + \cdots + v_{n-1}x + v_n$ and $g = g(x) = w_0x^m + w_1x^{m-1} + \cdots + w_m$ be two polynomials. Note that we are writing them in a nonstandard way, e.g. the leading coefficient is v_0 and the constant coefficient is v_n for a polynomial of degree n. We now form a $m + n \times m + n$ matrix M as follows: place the coefficients of f, starting with the leading term v_0 in the first row starting in the first column. Put zeros in the last $m-1$ places. In the second row we again place the coefficients of f, but now starting with 0 in the first column and v_0 in the second, v_n in the $n + 1^{st}$ column and zeros in the last $m - 2$ columns. Continue in this manner for the first m rows, each one starting one column later. The m^{th} row has v_n in the last column. Then starting with the $m + 1^{st}$ column we place the coefficients of g with w_0 in the first column through w_m in the $m+1^{st}$ column and zeros later. Continue the pattern down to the last row and w_m will appear in the last row, last column. For example, if $f = v_0x^3 + v_1x^2 + v_2x + v_3$ and $g = w_0x^2 + w_1x + w_2$ then M looks like

$$M = \begin{bmatrix} v_0 & v_1 & v_2 & v_3 & 0 \\ 0 & v_0 & v_1 & v_2 & v_3 \\ w_0 & w_1 & w_2 & 0 & 0 \\ 0 & w_0 & w_1 & w_2 & 0 \\ 0 & 0 & w_0 & w_1 & w_2 \end{bmatrix}$$

The *resultant* of f and g is $R(f, g) = \det M$, that is, the determinant of the matrix M. Note that the resultant is a number, not a polynomial.

In practice the best way to calculate the resultant is to use Maple. There is a procedure `resultant` with syntax `resultant(f,g,x)` to find the resultant of two polynomials with variable x. The coeffients of f, g can be numbers or variables or expressions.

We state the main theorem about resultants:

Theorem 1.13.1 *Let f, g be two real or complex polynomials. Then $R(f, g) = 0$ if and only if f and g have a common complex root.*

Actually, the idea of the proof is not too difficult and we will sketch it. First we need a refinement of Theorem 1.8.2.

Lemma 1.13.2 *Let $h = \gcd(f, g)$, then there exist polynomials u, s with $uf + sg = h$ with $\deg u < \deg g$ and $\deg v < \deg f$. u, s are unique if and only if h is a constant, i.e. f, g are relatively prime.*

Proof: By 1.8.2 there exist u, s with $uf+sg = h$. We need to show that we have the appropriate degrees. For example if $\deg u \geq \deg g$ then $u = gq+r$ where $\deg r < \deg g$ by the division algorithm, so $h = uf + sg = (gq + r)f + sg = rf + (gq + s)g$. But then $(gq + s)g = h - rf$ so $\deg g + \deg(gq + s) = \deg(gq + s)g = \deg(h - rf) \leq \max(\deg h, \deg rf) = \deg rf = \deg r + \deg f < \deg g + \deg f$ from which it follows that $\deg(gq + s) < \deg f$.

It is easy to see that u, s are unique if and only if the only solution to $uf + sg = 0$ with u, s of appropriate degrees is $u = 0, s = 0$. If f, g are relatively prime (i.e. h is a constant) the equation $uf = -sg$ requires g to divide u and f to divide $-s$ by an argument similar to that of Theorem 1.9.3 (or use the Unique Factorization Theorem). But this would violate the condition $\deg u < \deg f$ etc. If h is not a constant then $f = f_1 * h, g = g_1 * h$ where $\deg f_1 < \deg f$ and $\deg g_1 < \deg g$. But then $g_1 f = g_1 f_1 h = f_1 g$ so $g_1 f + (-f_1)g = 0$ showing non-uniqueness.

We now return to the proof of the theorem. The idea is to let the coefficients of u, s be unknowns and solve for them. So let $u = a_0 x^{m-1} + a_1 x^{m-2} + \cdots + a_{m-1}$ and $s = b_0 x^{n-1} + \cdots + b_{n-1}$. Form the expression $uf + sg$ and collect powers of x, note that each coefficient is a linear expression in the a_i, b_j with coefficients the v_i, w_j so to find u, s we can solve these $n + m$ linear equations in the $n + m$ unknowns $a_0, \ldots, a_{m-1}, b_0, \ldots, b_{n-1}$. It turns out that the matrix of this system is exactly the transpose of M. If f, g have no common roots then $\gcd(f, g) = 1$ so the system has a unique solution, and hence the determinant of the system (i.e. $\det M$) cannot be 0. Conversely, if f, g have common roots so $\gcd(f, g)$ is not constant and the equation $\gcd(f, g) = uf + sg$ has many solutions for u, s of the given degrees so the system is singular and thus has determinant 0.

In the case $g(x) = f'(x)$ then we have from 1.11.2

Corollary 1.13.3 *Let f' be the derivative of f. Then f has roots of multiplicity greater than 1 if and only if $R(f, f') = 0$.*

Finally we mention that if $f(x) = x^m + \cdots$ is monic then the number $R(f, f')$ is called the *discriminant* of f. We will meet up again with the discriminant in Chapter 4. For example let $f = x^3 + px + q$. Then one can easily compute (eg. via Maple) that $R(f, f') = -4p^3 - 27q^2$ which is exactly the discriminant that we will calculate in section 4.8.